RISCAuthority

administered by

FPA Fire Protection Association

Basic cyber security controls for the small business – awareness checklist

Version 1 Published 2016

IMPORTANT NOTICE

This document has been developed through RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

Contents

1 Introduction 4

2 ‘Cyber Essentials’ scheme 4

3 Awareness checklist 4

1 Introduction

This checklist is designed as a tool for the small business looking for some assurance (but not guarantee) that they have addressed the basic and essential cyber controls that a typical expert authority would expect to see in place in the smaller firm. That said, such a tool cannot exhaustively cover every eventuality as cyber risk profiles differ between businesses added to which cyber crime is constantly and rapidly evolving and mutating. Whilst the great majority of attacks are mounted by relatively less sophisticated individuals, more advanced or targeted attacks than this checklist addresses call for additional measures.

2 'Cyber Essentials' scheme

If you have already achieved the 'Cyber Essentials' or 'Cyber Essentials Plus' badge, your business should already have the controls that secure against 80% to 90% of the attacks mounted at the present time and you would be able to check off against this checklist with positive responses in most cases. However, if indeed you have taken your business through the 'Cyber Essentials' checklist process you will readily appreciate the danger of complacency, the need to monitor how cybercrime evolves and to ensure that your controls are subject to a continuous process of review.

FAQ

What is 'Cyber Essentials'?

Cyber Essentials is a Government backed scheme to help businesses protect themselves against cyber threat. Conformity to the scheme is essential for several kinds of government contract. Many large firms are now adopting Cyber Essentials and will increasingly expect the businesses in their supply chains to hold Cyber Essentials certification too. There is a choice of two routes to achieving this certification. The first, leading to achievement of the basic Cyber Essentials badge, being self assessment verified by an approved Certification Body; the second, leading to the Cyber Essentials Plus badge, being assessment by such a body itself – a more rigourous process generally rewarded with an enhanced level of recognition.

Search tip: navigate via https://www.gov.uk/government/publications and search for 'Cyber Essentials'

3 Awareness checklist

If the business is not certified against 'Cyber Essentials', how well defended is it taking account of the following?

Table 1: Checklist

		Tick
1.	Are you aware of the government's self-help tools: '10 Steps to Cyber security' document set and 'Cyber security: advice for small businesses' and have you adopted the recommendations? Search tip: navigate via https://www.gov.uk/government/publications and search for 'cyber security'.	□
2.	Is overall responsibility for cyber security assigned to a director or senior manager or an information and communications technology (ICT) security manager or similar dedicated role?	□
3.	Is information security routinely the subject of formal, and regular consideration collectively by all the partners, directors or, if applicable, the whole board? Are cyber crime trends monitored?	□
4.	Has your business:	
	Carried out a systematic analysis of the cyber assets that may be at risk? ***Examples:*** *IT physical equipment, confidential information, intellectual property, communications, procedures and processes*	□
	Mapped the flow and control of data a) within the business b) available to others outside the business? ***Examples:*** *Through contracted services or through legitimate or illegitimate use of access points*	□
	Considered the threats to the cyber assets? ***Examples:*** *Theft and malicious or unauthorised acts of all types (tangible and intangible assets), by criminals, cyber spies and vandals, employees, former employees, competitors, business partners, vendors and other third party service providers. Have you considered to whom your data is of most interest and assessed what their motivation might be for mounting an attack?*	□
	Estimated the impact of a cyber breach? ***Examples:*** *Financial loss from theft and disruption, damage to reputation, fines and litigation expenses, recovery costs. Consider which single event has the potential to impact your business the most.*	□

5.	In the context of the use that your business makes of cyber technology, has it implemented, and is it maintaining, all the basic precautions widely accepted as being fundamental to the security of every business, irrespective of size and sector? ***Examples:*** • the premises and ICT equipment are physically secure; • ICT equipment is under firewall protection; • wireless networks are suitably secure eg through use of 'WPA2'; • antivirus software with live update installed; • strong passwords are in use (eg per https://www.cyberstreetwise.com/passwords); • sensitive information is encrypted; • new versions of software, web browsers and software security patches are installed immediately they are available; • user privileges are restricted to the minimum required for each role; • business data is regularly backed up off site.	□
6.	Are there policies and measures in place to protect your network by denying unauthorised access that could result in its misuse, modification or undermining of its availability? This generally implies authorisation of access by strong authentication techniques, network segregation with clear 'air gaps' between distinct functions (eg industrial control *vis-à-vis* business processes) and might also mean that traffic on the network has to be encrypted.	□
7.	Through training and supervision, are your staff, to the extent necessary, familiar with, and updated on, cyber risk and do they have a role in its containment (eg reporting irregular access requests and attempts at 'phishing') and the detection of possible breaches?	□
8.	Have you tasked a credible in-house or outside expert (preferably an accredited ICT security professional) to assess your cyber risk and do you regularly implement 'penetration testing' with expert assistance?	□
9.	If expert recommendations have been made, have they been adopted?	□
10.	Are effective management procedures and damage controls embedded throughout the organisation that would limit and contain the impact of a breach such as the unsafe granting of access or release of data eg through a successful phishing attack?	□
11.	Do written cyber security policies exist eg covering 'bring your own device' (BYOD), use of removable storage (USB drives etc), access to inappropriate websites, use of social media?	□
12.	Are there ICT monitoring disciplines or software functions in place that would give early warning of any irregular or suspicious activity?	□
13.	Are cyber security controls subject to regular review, test and development?	□
14.	Does your business regularly review your governance policy and have you established whether, for example, you need to comply with personal data protection legislation and/or payment card industry compliance, with all necessary state-of-the-art controls in place?	□
15.	Are you satisfied that data stored or processed by vendors, eg specialised service providers and cloud services, is retained securely and protected against manipulation, leakage and theft?	□
16.	Do the contracts entered into with vendors fully protect and hold you harmless against claims that sensitive data have been inadequately controlled by that contracted party?	□

17.	Have response and recovery plans been developed for adoption in the event of a critical breach and are they regularly rehearsed and tested?	□
18.	With the benefit of having analysed your own cyber risk through this checklist (and similar tools), have you reviewed your overall risk exposure through revisiting the established high level principles of risk management, namely risk avoidance, risk reduction, risk retention and risk transfer and, in respect of the last of these, have you explored the role of cyber insurance with your insurance company or insurance broker?	□

RISCAuthority

administered by

FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk