Security solutions: Supporting you in achieving and maintaining Cyber Essentials/Cyber Essentials Plus

WHAT IS CYBER ESSENTIALS?

Cyber Essentials is a UK Government initiative to improve the cyber security of its supply chain by ensuring suppliers address the most common lines of technical attack experienced by government and industry.

THE RISK OF CYBER ATTACK

A UK Government survey[1] (2018) found that 43% of businesses and 19% of charities reported Cyber Security breaches. The same survey found that only 51% of small businesses and 29% of charities had implemented the 5 basic technical security controls that are recommended by the Cyber Essentials Scheme.

WHAT DOES CYBER ESSENTIALS MEAN FOR YOUR BUSINESS?

Cyber Essentials Certification is mandatory for organisations tendering for Government contracts which involve handling sensitive or personal information and providing certain ICT products and services.[2]

The Cyber Essentials Scheme consists of Cyber Essentials and Cyber Essentials Plus.

Both address the same controls:

- Cyber Essentials requires you to conduct a self-assessment of your organisation's IT against the Cyber Essentials Guidelines. This is reviewed by an accreditation body, which is authorised to issue the Cyber Essentials Certificate.
- Cyber Essentials Plus covers the same aspects as Cyber Essentials, with the key difference that it requires an independent review of your security controls. Consequently, Cyber Essentials Plus is more highly regarded by customers.

OUR APPROACH

The Cyber Essentials Scheme focusses on 5 key technical controls that help deliver cyber security. Computer systems are just one part of the complex system that you use to deliver your business to customers. This complex system includes your staff, ways of working, physical security and your computing infrastructure.

THE 5 CRITICAL SECURITY CONTROLS OF CYBER ESSENTIALS

- Firewalls
- Secure configuration
- User access control
- Malware protection
- Patch management.

Adversaries will seek to exploit any or all of these systemic components for their own ends.

Frazer-Nash can assist you to achieve Cyber Essentials, by using our experience of government and commercial security risk management to recommend a pragmatic approach to implementing the 5 key security controls within your business.

Our approach is to work with your organisation to understand your business and its priorities, in order to recommend pragmatic approaches to meeting the requirements of Cyber Essentials (technical controls).

In addition, we will look at the systems and processes surrounding your computer systems and recommend how common exploits may be prevented (systemic controls). This will help you maintain your Cyber Essentials Certification

WHY FRAZER-NASH?

Frazer-Nash Consultancy delivers security services to public and private sector clients, including Critical National Infrastructure (CNI).

We don't have a commercial interest in any particular method or approach. Because we don't sell Cyber Essentials Certification we can provide truly independent technical support, and apply our breadth of experience to assisting organisations to comply with cyber security frameworks.

[1] Cyber Security Breaches Survey 2018, Department for Digital, Culture, Media and Sport

[2] Procurement Policy Note – Cyber Essentials Scheme, Action Note 09/14, dated 25 May 2016, Crown Commercial Services.

For more information about Frazer-Nash please visit our website.
www.fnc.co.uk/security

www.fncaustralia.com.au

Offices throughout the UK and Australia

FRAZER-NASH CONSULTANCY