Loss prevention standards

Cyber Security:

Cyber Essentials Accreditation

This document provides guidance on Cyber Essentials, a UK Government-backed scheme designed to help organisations recognise cyber crime threats and how to assess their ability to protect against them.

AVIVA

Cyber Security:
Cyber Essentials Accreditation

Introduction

Cyber attacks and infiltrations aimed at all sizes of business and at individuals, have increased dramatically. Cyber criminals attempt to use any topical subject, including the COVID-19 pandemic, to prey on people and systems, whilst they are at their most vulnerable.

The Business Continuity Institute (BCI) in conjunction with the British Standards Institution publish their Horizon Scan Report annually. This report has been an indicator as to what businesses had seen as the biggest impacts on their organisation in the previous 12-months, and what their biggest concerns were for the coming year. The picture that this report provides is one where cyber attacks were previously a minor issue, but over the last few years they have become a large threat across all sectors and are now an organisations' biggest fear for the coming year. The 2020 Report shows cyber attacks and data breaches as the threats with the greatest likelihood to happen and the greatest potential impact. This clearly shows the concern businesses have.

To help businesses protect themselves against cyber crime, Aviva recommends Cyber Essentials Certification. Cyber Essentials is a UK Government-backed scheme designed to help recognise the threats and assess an organisations ability to protect against them.

The scheme will help businesses avoid, or at least minimise, the impact on their business of:

- Phishing attacks
- Malware
- Ransomware
- Password guessing
- Network attacks

Benefits of Cyber Essentials Accreditation

There can be many reasons to obtain accreditation. With cyber crime becoming a major threat to businesses across the globe, securing your IT and data and keeping your security measures and procedures up to date, will not only be essential for yourself, but could also give you a competitive edge in your market. It also helps to support your reputation and assure your data protection policies.

Having the accreditation:

- Gives you certified cyber security, from a UK Government-backed scheme
- Provides you with a clear picture of your organisation's cyber security level
- May assure your customers that you are working to secure your IT and data systems against cyber attack
- Means your organisation may attract new business given that you have cyber security measures in place

Some customers, going forward, may even require Cyber Essentials certification from their suppliers.

Obtaining Cyber Essentials Accreditation

Aviva have a Specialist Partner, CyberSmart, who provide a range of services and can provide Aviva clients with free advice, information and quotations.

CyberSmart were born out of a GCHQ accelerator in 2017. It was created by a group of forward-thinking security experts who noticed that many companies needed to secure themselves and achieve information security standards, but ultimately found the process too complicated or were limited by financial or human resources.

Their aim is to provide a much easier, quicker process to navigate, and their expertise has helped numerous businesses of all sizes.

Cyber Essentials Plus

For those organisations who want to improve cyber security further, there is Cyber Essentials Plus Certification. This is the highest level of certification provided by the Cyber Essentials scheme.

CyberSmart's market leading APP is used in Cyber Essentials accreditation. It is easily deployed and gets insights into the current security status of all devices which an organisation has.

To get accredited, the results of the CyberSmart APP are reviewed and acted upon, with guidance from CyberSmart. The APP itself then checks every 15 minutes to ensure users and devices remain compliant and a weekly report is produced.

In addition to the self-assessment, Cyber Essentials Plus includes a technical audit to verify the results. An assessor would select a representative sample of devices to audit.

How Does Cyber Essentials Work?

Cyber Essentials sets out 5 controls which can be implemented immediately to strengthen cyber defences:

1. Firewall - use a firewall to secure your internet connection
2. Settings - choose the most secure settings for your devices and software
3. User Privileges - control who has access to your data and services
4. Protections - protect yourself against viruses and malware
5. Updates - ensure the latest updates for devices and software are installed, these include security updates

Following this, accreditation can be issued and businesses choosing CyberSmart will have the added security of the CyberSmart APP monitoring their systems, users and devices for compliance.

As cyber crime is becoming more common place and cyber criminals being anything from an organised group to an individual, with attacks from anywhere in the world, it is essential to protect your organisation's, your customer's and your supplier's data and sensitive information.

With Cyber Essentials accreditation, proof and assurance can be provided to business partners, to existing and prospective customers and to any other interested parties, that your organisation is proactively guarding against cyber attack.

The protections implemented can be essential in protecting against cyber attacks. With CyberSmart's APP and the monitoring it provides, it will help maintain the protections required to be in place and ensure they are up to date in the battle against cyber crime.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- CyberSmart
- The National Cyber Security Centre
- ActionFraud

Additional Information

Relevant Loss Prevention Standards include:

- Pandemic Planning & Coronavirus
- Pandemic Recovery: 'New Normal' and the Post-Pandemic Business World
- Cyber Security – Top 12 Tips to Protect Against a Cyber Attack

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*Calls may be recorded and/or monitored for our joint protection.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

17/08/20 V1.0

LOSS PREVENTION STANDARDS