Article

Jun 2022

The right frame of mind

As the use of online tools increases for communication, data storage and sharing, and automation, so do the opportunities to attack them.

Kieran Fowler
Head of Cyber Consulting

Email kieran.fowler@waterstons.com

39% of all UK businesses experienced a cyberattack in the last 12 months. That's an immeasurable amount of data, revenue and innovation breached – and possibly ransomed – that could easily have been protected.

What tools are available to protect and support your business from, and in the event of, a cyberattack? You need a framework.

What is a framework?

Simply put, it is a set of best practices put in place and followed across an organisation to manage any cybersecurity risk.

While in place to ideally reduce a firm's exposure to cyberattacks through identifying the areas and data most at risk, frameworks can also help teams understand the actions that need to be taken if defences are compromised.

Becoming cyber resilient is not a one-time activity, it's a journey that organisations will increasingly need to embark on to a lesser or greater extent through the dynamic and developing cybersecurity landscape, and there are a number of frameworks that support that.

A framework should not stand alone however and must be closely linked with risk management strategies and procedures, as well as other key areas of a business.

Here we share some of the most common cybersecurity frameworks that can support your business to help find the best one for you.

ISO 27001

Seen as the Gold Standard across the world when it comes to information security best practice, this provides a holistic way to identify, assess and reduce information security risks right across your organisation's environment.

The framework helps produce a comprehensive information security management system (ISMS) and as part of the process, companies are required to identify information security risks and select appropriate controls to tackle them.

Not only will ISO 27001 help protect an organisations data, it'll help meet contractual obligations, legal GDPR requirements and build in a secure organisational culture from the ground up.

National Cyber Security Centre (NCSC)

The NCSC have developed their Cyber Assessment Framework (CAF) with the security of UK organisations in mind. It puts a particular focus on essential business functions that would have a direct impact on the infrastructure of the UK from the economy to individuals' welfare.

The NCSC understands UK industries can be very different and there is no, one, all-encompassing guide, when it comes to cyber security. Therefore, the CAF is written around 14 cyber resilience principles that have broad goals around good cyber security practice.

This really distinguishes the CAF from other frameworks that could be seen as more generic compliance checklists.

Cyber Essentials

Cyber Essentials is a framework backed by the UK government and supported by the NCSC. It has 5 basic security controls that can protect organisations against 80% of common cyber threats.

Cyber Essentials can be completed as a self-assessment and the approach is very simple and cost effective, so the scheme is of particular value for small to medium sized organisations.

Being Cyber Essentials certified not only protects organisations from cyber-attacks, but it helps secure new business opportunities and also demonstrates a basic level of cyber maturity in organisations supply chain.

While there are many frameworks available in the cybersecurity space, it's important to find out what is best for your business, your industry and your team.

Speak to a cyber security expert to find out how you can be continually protected against cyberattacks today.