Case study

Sector Architects, Engineering & Construction
Service Cyber Security

May 2021

Cyber Essentials: The springboard to your security journey

Cyber Essentials is steadily gaining traction in many sectors as a baseline security requirement – but what is it, how is it implemented and what are the benefits to your organisation?

Iain Batty
Technical Security Assessment Lead
Email iain.batty@waterstons.com

Results at a glance

- Cyber Essentials accreditation
- Cyber Essentials Plus accreditation

The Challenge

With constant news of household names being compromised by hackers and nation-states crippling organisations with ransomware and phishing attacks, the rush to batten down the hatches has begun, with every vendor selling their 'magic talismans' of security appliances and certifications to allay your every fear, of which they tell you, there are many.

This fearmongering can be counterproductive. All the noise makes it difficult to know where to start and many organisations are reticent in taking their first steps and are anxious that tighter security will mean more red tape and less efficiency. Additionally, certifications, particularly ISO 27001, can be significant undertakings with a typical implementation duration of around 12-18 months. The expense and impact of such an endeavour is more than many organisations are able to commit to, especially if security is a new initiative and they're taking their first steps towards addressing risk. Some organisations may also already have good security practices in place, but the cost of validating this with certification discourages them from doing so.

However, a large number of organisations, regulators and government bodies now mandate specific security requirements within their chain of suppliers or member organisations, to ensure that those with access to their data or systems don't introduce weaknesses into their information security. They require specific certifications that align with the risks and strategic focus of their associated sector, so that a baseline of security is established to ensure safe business practices.

Jestico + Whiles, an award winning architectural firm and interior design practice based in London, decided to seek certification to demonstrate their commitment to information security and attain a competitive edge for developing new opportunities.

The Solution

Cyber Essentials and Cyber Essentials Plus are achievable, entry-level certifications that address the most common risks to businesses in the UK; malware infections and automated internet-borne attacks.

The framework focuses on five controls to implement a standard of security:

Boundary firewalls and internet gateways

Devices that connect an organisation's systems to the internet are the first line of defence against external threats. Consequently they have to be properly configured to provide the smallest attack surface possible, while still providing key business services to those that are authorised to use them.

Secure configuration

To reduce the possible attack vectors and avoid disruption to key business processes, systems and applications need to be properly configured in a way that is secure and tailored to the organisation's requirements.

Access control

Limiting access to systems and data to individuals that have a validated business need and only to the level they require to fulfil their role.

Malware protection

Protecting systems from malware infection or untrusted applications via effectively configured and updated anti malware software across the organisation.

Patch management

To avoid the exploitation of new vulnerabilities and ensure consistent patching is enforced across all in-scope devices and systems. A key requirement here is that all in-scope systems must still be in support, Windows Server 2003 and XP installations are common pitfalls for organisations attempting to satisfy this requirement.

> **Waterstons took the time to understand our infrastructure and how we operate as a business, allowing them to provide a clear and effective roadmap to certification that was achievable and specifically tailored to us.**
>
> Darren Carroll
> Head of IT

The key point here is that these controls are simple and attainable – usually with systems already in place within an organisation. We delivered a two day 'gap analysis' after which Jestico + Whiles were able to use the findings as a roadmap for their own risk treatment plan, implementing and testing solutions unaided in preparation for the certification audit by our Cyber Resilience Team. They leveraged the functionality of systems already in place, such as Web Content Filtering on their firewall appliances and Mobile Device Management functionality present in a system already in place, to address the framework's specific requirements.

Following that they then pursued certification, of which there are two possible levels:

Stage 1 - Cyber Essentials: Self-assessment questionnaire of in-scope systems independently validated by an accredited third-party.

Stage 2 - Cyber Essentials Plus: An additional technical assessment of security controls of in-scope systems that validates the effectiveness of implemented security controls.

The Benefits

By attaining both Cyber Essentials and Cyber Essentials Plus certification Jestico + Whiles have an assurance that they're well protected against the most common attacks aimed at businesses in the UK. Through collaborative effort with us, they achieveed Cyber Essentials within a matter of months, using the functionality of systems already in place and with minimal impact to users. Other organisations following a similar journey may have to invest in additional security controls to meet the requirements, but achieving certification is a low cost and high value safeguard against the cyber threats of today.

Certification has also opened up doors for Jestico + Whiles to engage with an array of government bodies and other organisations on new tender opportunities. Their early adoption of the certification is a key differentiator in an industry that will soon require it to be a supplier prerequisite.

Re-certification is required every year, meaning the efforts implemented will be annually re-evaluated for their effectiveness. This embeds the concept of continual improvement into Jestico + Whiles' IT Strategy, by ensuring they are routinely assessed to confirm that new vulnerabilities haven't been introduced into their infrastructure. Consequently, this shift towards forward thinking information security will act as a key business driver for change, and as the organisation grows, will put them in a strong position to pursue further certification such as ISO 27001.

Certification proves to our customers that we strive to deliver excellence both in our services and how we operate as a business – this improves confidence in our business practices and provides a world of opportunities that were previously out of reach.

Darren Carroll
Head of IT