HOW A MID-SIZED SERVICE PROVIDER SECURED THE COMPETITIVE EDGE

The Business Challenge

Among our customers, it is reassuring to find that cyber security is increasingly becoming the responsibility of the most senior level of the business. Of course, what our customers are finding is that cyber security is also becoming a priority to their own customers, with many insisting they comply to a range of standards before they can be considered as a potential supplier.

In this instance, a mid-sized public sector service provider, dealing with a number of public sector contracts, needed to achieve Cyber Essentials (CE) certification to meet specific assurances for a number of customers before they could make a coveted pre-approved supplier list.

This organisation had limited IT resource and certainly no cyber security team to understand exactly what was required of them. What they did understand was that their competitors, as early adopters to the CE scheme, were gaining a market advantage by demonstrating their cyber security protection.

The Solution

Cyber Essentials projects are generally quite short, tailored to the size of the organisation. The main focus is on cyber security breach prevention, and doing sensible things that are known to work. It doesn't normally involve significant investment in new security systems and never requires additional staffing.

A focus on the external internet firewall uncovered significant vulnerabilities associated with systems that shouldn't have been exposed to potential hackers. This was a good example of IT 'making it work', without knowledge of the security implications. These weaknesses were corrected, with an appropriate firewall configuration quickly developed by Daisy and implemented.

As most CE customers have not undertaken in-depth cyber security penetration testing, they are often unaware of technical vulnerabilities. The CE requirement for vulnerability scanning is a great starting point to show where technical weaknesses are present. The remediation of these vulnerabilities usually involves the introduction of a more rigorous approach to system patching and secure system configuration. This process helps the IT team understand the importance of these processes in breach prevention.

Further analysis also showed many legacy access controls, with previous users retaining access with weak password controls. These were quickly corrected, as ex-employees can pose a significant risk.

Through introducing these controls, the senior management team started to understand the importance of the improvements, and appreciated the cost-effective approach of CE. They are now looking at a wider ISO 27001 certification programme, to give wider control of information security. This will help with their future GDPR compliance and open up further sales opportunities.

Benefits

- Uncovered significant vulnerabilities associated with systems
- Improved sales prospects thanks to achieving a new certification
- The customer's end users, stakeholders and their own customers have greater confidence in them
- Greater levels of cyber security protection, with no additional staff required
- Internal education and increased knowledge for IT team

AT A GLANCE

Industry sector:
Public Sector Service Provider

Solutions/services taken:

- Cyber Essentials
- ISO 27001

Length of Relationship:
6 years

*The initial engagement was with ECSC, acquired by Daisy in 2023.