SWANSEA BAY UNIVERSITY HEALTH BOARD | CYBER ESSENTIALS+

Scoping for scalable success with Cyber Essentials+

Until recently, Swansea Bay University Health Board was most familiar with Cyber Essentials+ as a requirement for organisations they engaged with. This time, Swansea Bay UHB was the customer in a contract to provide vocational training for apprentices. Securing the contract depended on CE+ certification. Budget approval was easily achieved – the question was, how would Swansea Bay UHB define the scope to meet the requirements set out by Cyber Essentials+ to meet a tight deadline?

We spoke to Gareth Ayres, Cyber Security Manager, Swansea UHB to get his firsthand account of this CE+ success story.

1

Get set up to succeed
It's been a really valuable experience to achieve CE+ for this smaller scope initially. We've gained a better understanding of what the certification actually requires, and we've rolled out a number of policy and technical changes directly as a result of lessons learned.

2

Integrate with the rest of the business
Ultimately, everyone in the organisation shares the same objective to enable patient care. But while we're united on that front, it's not unusual for the ideals of the cyber security function to jar with what's possible in reality. In this instance the contract would have been lost without the certification. The process involved working with some areas of IT to complete the assessment focused on end-user devices – this resulted in a great example of cross-functional cooperation. Acknowledge the opportunity to connect with Board-level directors in completing this kind of project, because it might just be a chance to boost the cyber security team's reputation internally as business enablers. Our direct line to the Director of Digital has definitely strengthened thanks to CE+.

3

Invest in the right kind of expertise
The benefits of working with a consultant is their expertise in the specific requirements and the certification itself. In this example, it doesn't matter how technically savvy you are, a consultant like Stratia Cyber knows exactly what to look for and is able to give guidance on how to get ahead and implement appropriate changes.

Clinical staff on the front line see the direct impact in the event the IT system goes down.

Gareth added: “Inside and outside of this assessment, it’s difficult to put additional pressure on staff to take on more cyber security responsibility. The fact of the matter is, we all need NHS digital services and systems to be secure in order to achieve what we set out to do. Risk appetite in the NHS is much lower than other sectors, and this can represent an obstacle when it comes to implementing change.

The good news is, the wider workforce are much more aware of the impact of a cyber attack than they were a short time ago. No one wants the IT system to go down, especially clinical staff on the front line who can see the direct impact in the event of out outage.

“The most realistic progression path for an organisation like the NHS is to start small. We were pleasantly surprised when we discovered we could scope down, customise things, and rule out chunks of the infrastructure for this project. There are multiple benefits to adjusting the scope – we know for a fact that if we attempted to achieve CE+ on a global scale we’d fail.

Previously, it had never been a business requirement to obtain CE+ – NIS compliance is top priority because it’s required by the Welsh Government. Cyber Essentials+ builds a level of assurance, and our long term goal is to achieve certification for the whole health board.

In the meantime, our aim is to get funding to certify the Cyber Security team itself and be in a position to lead by example.”