Funding boost to help healthcare suppliers improve cyber security

Hundreds of the country’s vital healthcare firms are set to benefit from government funding to boost their cyber security, the Digital Infrastructure Minister Matt Warman announces today, as part of London Tech Week.

The move comes after the National Cyber Security Centre (NCSC) identified a heightened cyber threat to the UK health sector in relation to the pandemic, with cyber crime groups attempting to steal sensitive intelligence, intellectual property and personal information from pharmaceutical companies and medical research organisations.

Small and medium-sized businesses, such as medical suppliers and primary care providers, are being invited to apply for a slice of the £500,000 funding for the initiative which will see all consultancy and certification costs covered by the government.

Participants can receive guidance and support to get accreditation from the government’s Cyber Essentials certification. This includes training to make sure all phones, tablets, laptops or computers are kept up-to-date, proper firewall usage to secure devices’ internet connections, and user access controls to manage employee access to services.

Firms could opt to receive support from one of the programme’s cyber experts, who will look at the organisation as a whole, identify its cyber security risks and help develop and implement a business continuity plan.

Digital Infrastructure Minister Matt Warman said:

> We know there is a heightened cyber threat for healthcare businesses at the moment so we are releasing new funding to help those playing a vital role in the pandemic response to remain resilient.
>
> I also urge all organisations to sign up to the government’s Cyber Essentials programme which contains a number of simple steps firms can take to get the fundamentals of good cyber security in place.

Paul Chichester, the NCSC’s Director of Operations, said:

> Protecting healthcare has been our top priority during the Covid-19 pandemic and we have been working hard to ensure organisations can keep themselves secure.
>
> While we will continue to support them, signing up to initiatives such as Cyber Essentials is an excellent way for organisations to

> help themselves.
>
> Those who have not already taken up this offer should do so – it will help ensure they have fundamental security protections in place, even in the most challenging of times.

Despite good progress in recent years, almost half of all businesses (46 per cent) suffered a cyber breach or attack in the last 12 months, with one in three per cent (32 per cent) experiencing them at least once a week, according to the Cyber Security Breaches Survey 2020.

Recent graduates of the Cyber Essentials programme include an app development firm whose products have supported Covid-19 patients and clinical teams throughout the pandemic, a not-for-profit organisation offering vital youth programmes to disadvantaged young people across the North East, and a group providing accessible health services across Yorkshire during the Covid crisis.

A Cyber Essentials participant from the healthcare sector said:

> As a key supplier of medical equipment to the NHS, we qualified for government funding for a Cyber Essentials check on our IT systems. It was simple to arrange, we found the assigned partner easy to work with and overall the service has been an excellent sanity check on our IT systems and processes to ensure we are working to the best current security practices. It is definitely worth doing if you can.

This announcement comes on the day the London Office for Rapid Cybersecurity Advancement (LORCA), the government-backed cyber innovation programme, reveals companies supported by LORCA have raised more than £150m in investment since it launched two years ago, more than triple the original target and 12 months ahead of schedule.