outsource
www.outsourcemagazine.co.uk

Getting the basics right: the UK government's new Cyber Essentials Scheme

Spurred on by its analysis of cyber attacks against UK enterprises, the government has identified a series of basic technical controls that many businesses are failing to use to manage cyber risk. Whilst that might not come as a surprise, the government response to it will certainly attract the attention of the outsourcing industry. The Cyber Essentials Scheme is coming, setting out ways to demonstrate cybersecurity that will become a requirement in government procurement contracts and may well determine how available, and expensive, cyber insurance cover is.

The Cyber Essentials Scheme was released on 7th April with a consultation phase ending on May 7th, and the Scheme will be launched on 5th June. It describes a set of controls that businesses, large or small, can set up in order to achieve a minimum standard of cybersecurity and the government wants it to be widely adopted. To be clear, the Scheme is not a new standard (although it builds on aspects of ISO27001); instead it sets out a procedure for businesses to build a basic resistance to cyberattack and then have that resistance externally certified. This external validation is an important element: it should enable customers – crucially, of course, H.M. Government – to be assured that a supplier meets a measurable standard of cyber risk management. It is likely to have other implications too. From a legal point of view, there will be a more accessible standard against which directors and boards may be held accountable: cyber risk management is very much a governance issue. Also, the new regime may become a de facto benchmark for business to business dealings, lending itself to assessment of performance and even determination of negligence. The way in which the insurance industry recognises the certification in policy requirements and premiums will also affect take-up.

The government has said that it will use the Scheme in procurement contracts where that use would be relevant and proportionate. It seems that there will first be an assessment of the benefit of adoption in each contract area and then advance notice of implementation of requirements, to give tendering parties time to acquire the necessary level of certification.

To give an idea of how the Cyber Essentials Scheme would work, here are the five areas which it addresses:

- Secure configuration for computers and network devices, to reduce unnecessary vulnerabilities.
- Boundary firewalls and internet gateways to provide, at minimum, a basic level of protection where an organisation connects to the internet.
- Control of access and administrative privilege management: protecting user accounts and helping prevent misuse of privileged access.
- “Patch” management to ensure that the software used on computers and network devices is kept up to date.
- Malware protection against a broad range of threats and the capability to carry out virus removal.

Once the Scheme is running, any business will be able to get the certificate or ‘badge’ showing which level it has attained. The government does not propose to administer this programme, but instead will look to outside entities, starting with a series of accreditation bodies that will be set up. These will have the power to license certification bodies. The certification bodies will be the ones that assess and certify businesses, and if appropriate award them a “badge” of compliance. There are going to be three levels of certification: Bronze, based on a self-assessment; Silver, based on an independently verified testing process; and Gold, based on an independently verified testing process plus an “audit”. The Bronze and Silver levels only provide snapshots of an organisation at one moment in time; the Gold level additionally audits governance and processes to measure the sustainability of the process.

There are areas which have yet to be resolved, and some additional clarity can be expected at the June 5th launch. What will not be clear at the outset, but is contemplated in the Scheme, is the treatment of external cloud platforms – especially when businesses use cloud resources to carry out business-critical functions using company data. This is a developing area – and one that offers great promise of improved efficiency. However, the terms on which cloud services are bought and used are critically important and can clearly impact on cyber risks.

The Cyber Essentials Scheme has been devised for mass adoption because of the government’s concern that many companies, and indeed other organizations, are lagging behind in basic cyber security. It is acknowledged that cyber risk management and governance are more difficult for smaller organizations, but larger ones can be lax in basic precautions too. The use of procurement requirements will undoubtedly help to drive adoption given the scale of the government’s buying power, particularly in the IT sector. Although the roll out of procurement requirements will be a phased one, companies will want to reflect on the fact that the underlying elements of the Cyber Essentials Scheme are already capable of implementation, and that there are external advisers who are able to help not only with the design of compliant systems, but also the monitoring of them. They just can’t give you the badge yet.

Author: Nigel Montgomery, Partner, Sidley Austin LLP

Article reproduced with permission of Outsource; first published on www.outsourcemagazine.co.uk on May 19, 2014