Ensuring your organisation is safe from a cyber-attack and reducing the cyber risk in 10 critical areas: An Informative guide

Words Worth Reading Ltd: July 2015

"Both professionally and privately, we are all increasingly more aware of the value of information, and why others might want to access it, using fair means or foul. Given the environment in which healthcare organisations operate, the complexity and criticality of IT systems and the volume of confidential data that is held, the exposure to cyber risk is significant and therefore assurance is needed that adequate protection exists." – *Baker Tilly, 2014*

All organisations need to be aware of the risks associated with cyber-attacks, and work to ensure that they have mechanisms in place to protect against such attacks occurring. As highlighted above, this is particularly important for healthcare organisations, because of the level of risk that is associated with such organisations. In recognition of this heightened risk, the Information Governance Toolkit (version 13 onwards) asks that all healthcare organisations, either NHS or those that work with the NHS in any capacity, are able to demonstrate assurance of cyber-attack protection strategies.

This summary document outlines the most holistic way to approach cyber security, and identifies the 10 Steps to Cyber Security that were put forward by the Cabinet Office earlier this year.

A Holistic Assessment of your Cyber Security Management

Identifying an organisation's risk of cyber-attack is often best approached from a risk management perspective, which means taking a holistic assessment of the likelihood of systems being attacked and held information being lost. The completion of a Cyber Risk Health Check can be very useful here.

A Cyber Risk Health Check is the process of assessing the vulnerability of an organisation's IT systems and processes. The following areas should be considered:

> *The performance of a Cyber Risk Health Check should form part of your corporate governance framework and also help to provide assurance that the key components to help prevent a successful cyber-attack are in place.* – *Baker Tilly, 2014*

1. **Cyber Security Strategy**: Is there an over-arching strategy in place?

2. **Security Policy and Responsibilities**: Do in-house security policies include references to cyber risks and mitigation processes?

3. **Cyber risk education processes**: How are staff educated about how to recognise and respond to cyber risk?

4. **Software Updates**: Is there a process in place for ensuring that all devices complete their software updates when prompted? Do staff realise the importance of this?

5. **Cyber fraud prevention**: What oversight is in place to provide assurance that there are no concerns over internal cyber fraud?

6. **Vulnerability testing**: How frequently is the security of your network and systems tested?

10 Steps to Cyber Security

In 2012 the Government Communication Headquarters (GCHQ) originally published guidance on how businesses can protect themselves in cyberspace. Around two thirds of the FTSE350 now use this guidance to inform their cyber security strategies and practices. In 2015 the guidance around cyberspace protection was re-released, and the Information Governance Toolkit reflected the need for health and social care organisations to respond to this guidance, through adherence with The 10 Cyber Security Steps.

What are these 10 Cyber Security Steps?

Information Risk Management Regime ▪ Establish a governance framework ▪ Determine your risk appetite ▪ Maintain the Board's engagement with cyber risk ▪ Produce supporting risk management policies ▪ Adopt a lifecycle approach	**Secure Configuration** ▪ Develop corporate policies to update and patch systems ▪ Create and maintain hardware and software inventories ▪ Lockdown operating systems and software ▪ Conduct regular vulnerability scans
Network Security ▪ Police the network perimeter ▪ Protect the internal network ▪ Monitor ▪ Test the security controls	**Managing User Privileges** ▪ Establish effective account management processes ▪ Limit the number and use of privileged accounts ▪ Monitor all users
User Education and Awareness ▪ Produce a user security policy ▪ Establish a staff induction process ▪ Maintain user awareness of the threats ▪ Support the formal assessment of IA skills	**Incident Management** ▪ Obtain senior management approval and backing ▪ Establish an incident response and disaster recovery capability ▪ Provide specialist training
Malware Prevention ▪ Develop and publish corporate policies ▪ Establish anti-malware defences across the organisation ▪ Scan for malware across the organisation	**Monitoring** ▪ Establish a monitoring strategy and supporting policies ▪ Monitor all ICT systems ▪ Monitor network traffic

Removable Media Controls	Home and Mobile Working
▪ Produce a corporate policy ▪ Limit the use of removable media ▪ Scan all removable media for malware	▪ Assess the risks and create a mobile working policy ▪ Educate users and maintain their awareness ▪ Apply the secure baseline build

The Cyber Essentials Scheme

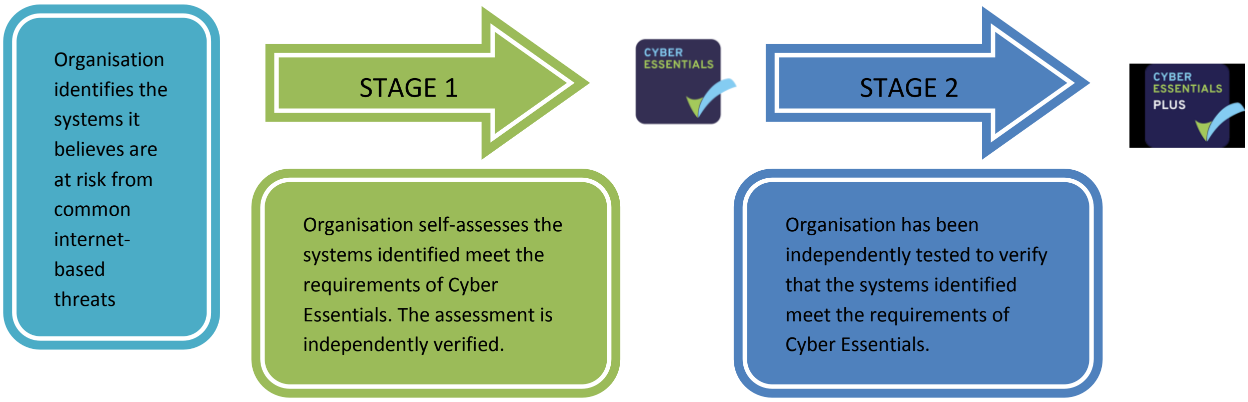
The Cyber Essentials Scheme was developed by Government and industry to provide an Assurance Framework through which organisations can demonstrate to customers, investors, insurers and others that they have taken the essential precautions outlined in the 10 Steps to Cyber Security.

A self assessment toolkit is used as part of the Assurance Framework, allowing organisations to record how they have successfully responded to the 10 Steps to Cyber Security. This leads to the awarding of the Cyber Essentials and Cyber Essentials Plus certificates for organisations.

The Assurance Framework focuses on five key controls:

1. **Boundary firewalls and internet gateways** – these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
2. **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organisation.
3. **Access control** – Ensuring only those who should have access to systems have access and at the appropriate level.
4. **Malware protection** – ensuring that virus and malware protection is installed and is it up to date.
5. **Patch management** – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor have been applied.

The awarding of the Cyber Essentials and Cyber Essentials Plus certificates can be achieved as follows:



Organisation identifies the systems it believes are at risk from common internet-based threats

STAGE 1

Organisation self-assesses the systems identified meet the requirements of Cyber Essentials. The assessment is independently verified.

STAGE 2

Organisation has been independently tested to verify that the systems identified meet the requirements of Cyber Essentials.

Words Worth Reading Ltd would recommend that all health and social care organisations seek to achieve a Cyber Essentials Certificate in 2015/16.

How Words Worth Reading Ltd can help...

Words Worth Reading Ltd are leading experts in the completion of successful Information Governance Toolkit assessments for health and social care providers, and for SMEs providing information and analysis-based functions for the NHS. We recognise the importance of an integrated approach to assessing the true risk posture of your organisation. We have a dedicated Information Governance team who provide a variety of services to help manage the risks to your organisation, and also support the completion of all Cyber Essentials assessments. Services include:

- Full Cyber Risk Health Check completions

- Cyber security strategy and policy creation

- Creation and delivery of bespoke training for staff

- Internal cyber fraud prevention policy and process creation

- Full support package for the completion of the Cyber Essentials certification assessment / application

http://wwwwordsworthreading.blogspot.com/

www.wordsworthreading.co.uk

www.twitter.com/WordsWorthR

www.facebook.com (search for Words Worth Reading)