HM Government

Cyber Security Organisational Standards

A call for views and evidence

March 2013

Contents

Overview: cyber security strategy and standards 3

Key dates 4

How to respond 4

Requirements for an organisational standard for cyber security 5

References 5

Purpose 5

Definitions 5

Applicability and Relevance 5

Ownership 5

Requirements for an Organisational Standard for Cyber Security 6

Overview: cyber security strategy and standards

Government published its Cyber Security Strategy[1] in November 2011. This set out our intentions to encourage industry-led standards and guidance that are used by organisations to manage the risk to their information, and to encourage companies that are good at managing information risk make this a selling point for their business. This call for evidence, and our subsequent selection of a preferred standard, will help companies identify what good cyber risk management looks like and select which organisational standard to invest in.

Cyberspace is vital for the UK's economic prosperity, national security and for our way of life. It brings many opportunities for businesses and consumers, but also threats from cyber crime, espionage, and terrorism, which must be addressed. The loss of - or damage to - information, can have a significant impact on an organisation and on the broader UK economy. Whether that loss is by accident or through malicious attack, the outcome is the same; risk to brand and reputation, financial risk, risk to growth potential.

Effectively managing the risk to its information should be a core part of any organisation, big or small. The average cost of a small business' worst information security breach in 2012 was £15,000-£30,000, and of a large organisation's, £110,000-£250,000. Information security breaches cost the UK economy billions each year.[2]

[1] https://www.gov.uk/government/publications/cyber-security-strategy
[2] PwC 2012 Information Security Breaches Survey

Key dates

We welcome your expression of interest to submit evidence in support of your preferred standard by **Monday 8 April 2013**.

We will then publish guidance for submitting bodies by **Tuesday 30 April 2013**.

The final date for submitting evidence will be **Monday 14 October 2013**.

How to respond

To notify us that you wish to submit evidence in support of your preferred standard, you can contact us using these methods:

Email: cybersecurity@bis.gsi.gov.uk

Post: Cyber Security Team
BIS
1 Victoria Street
London
SW1H 0ET

Please include:

1. the name of your industry body or group of companies; and
2. the name of the standard against which you intend to submit evidence.

Requirements for an organisational standard for cyber security

References

a. ISO/IEC 27032: 2012, Guidelines for Cyber Security.
b. Cyber Security Guidance for Business and the 10 Steps to Cyber Security, https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

Purpose

1. The purpose of this document is to articulate a series of requirements that Government judges a 'good' organisational standard for cyber security should look like. Government will use these requirements to select and endorse a preferred organisational standard amongst the private sector.

Definitions

2. For the purposes of this document, terms are used in accordance with the definitions in reference (a) above, including:
    a. Cyber security; preservation of confidentiality, integrity, and availability of information in cyberspace.
    b. Cyberspace; complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.[3]

Applicability and Relevance

3. These requirements are applicable to bodies or organisations that develop, use, or want to use organisational standards for cyber security.

4. Managing the risks from Cyberspace is relevant to organisations of any size that interact with the Internet.

Ownership

5. These requirements are owned by HMG.

[3] For the purposes of this document, components of cyberspace, such as routers and cables, do exist in physical form.

Requirements for an Organisational Standard for Cyber Security

6. The organisational standard should:
    a. Protect organisations of all sizes against low-end methods of compromise, such as phishing and social engineering, malware and viruses.
    b. Have in place, or will have in place, an independent audit and assurance framework.
    c. Be recognised or aligned internationally, or there will be a clear path to international recognition or alignment.

7. The organisational standard should be designed to deliver the following outcomes when correctly implemented:
    a. Responsibilities for managing cyber security risks are owned by the Board and are assigned to directors, managers, and other individuals, who can be held to account if they fail to meet their responsibilities.
    b. There is confidence that the controls in place mitigate the risks posed from low-end methods of compromise.
    c. People working in or for the organisation act in accordance with a code of ethics that promotes trust in their commitment to cyber security for the long- term good of the organisation.
    d. In the event of cyber security incidents, Boards and directors should be able to demonstrate due diligence in the opinion of the authority that appoints them.

8. To achieve the above outcomes, the organisational standard should include auditable requirements for the following technical and non-technical controls:
    a. The governance of cyber security across the legal entity including dependencies upon other organisations.
    b. The understanding of cyber security risks based upon the likelihood of the low-end methods of compromise exploiting vulnerabilities and causing business impacts.
    c. The selection of controls to mitigate cyber security risks using an appropriate mix of awareness, preventative, detective and recovery controls across the physical, personnel and technical security functions.
    d. The selection of controls should cover at least the following areas as described at reference b:
        i. Network security
        ii. Malware prevention
        iii. Secure configuration of information systems
        iv. Monitoring
        v. Removable media
        vi. Home and mobile working
        vii. Managing user privileges
        viii. User education and awareness
        ix. Incident management

e. Monitoring of the threat landscape and the effectiveness of the controls against that landscape.
f. The ability to react to changes in understanding of cyber security risks.
g. Reporting cyber security performance and incidents to the organisation's owners, customers, information owners and regulatory authorities, in a structured manner that enables monitoring of cyber security trends across industry and identification of root causes of incidents.

9. The organisational standard should not contradict legal or regulatory requirements relating to cyber and information security.

10. The organisational standard, its ownership, and the process for submitting and handling of requests for change should be made publicly available.

This publication is also available on our website at www.bis.gov.uk
Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

URN BIS/13/659