Cyber security organisational standards: call for evidence

Department for Business Innovation and Skills

This is an Engineering the Future response to the Business Innovation and Skills Cyber security organisational standards: call for evidence.

The development of this response has been led by:

- **The Institution of Engineering and Technology**
- **BCS, The Chartered Institute for IT**

The response has been written with the assistance of and endorsed by:

- The Royal Academy of Engineering

14 October 2013

For further information please contact:

Thomas Man, Engineering Policy Manager, The Royal Academy of Engineering

thomas.man@raeng.org.uk 020 7766 0654

Engineering the Future is a broad alliance of engineering institutions and bodies which represent the UK's 450,000 professional engineers.

We provide independent expert advice and promote understanding of the contribution that engineering makes to the economy, society and to the development and delivery of national policy.

The Institution of Engineering and Technology

The Chartered Institute for IT
Enabling the information society

This response to the BIS call for evidence on cyber security standards has been drafted by the IET and the BCS on behalf of the Engineering the Future alliance (EtF), and is supported by the Royal Academy of Engineering.

In summary the alliance's position on the call for evidence is as follows:

1. It is not possible to have a single standard for cyber security that is suitable for all organisations and able to deal with all eventualities. Such an approach over simplifies the complexity of the issue and the scale of the challenge.
2. EtF has been involved with the Industry Working Group and is broadly supportive of their **framework approach** to cyber security standards. Although like many in the group, we see current draft response as a minimum interim guide that might be used to help inform SMEs/micro SMEs around some aspects of cyber security and what steps may be taken to identify gaps and vulnerabilities. The document attempts to outline steps that may be taken based on good practice recommendations from the IASME organisation.
3. The alliance strongly believes that government should undertake a systematic approach that considers not only the **symptoms** but also the **root causes**.

Engineering the Future is offering to help government consider the challenges around cyber security and has identified the following potential workstreams that we could partner with government on.

In relation to the addressing the **symptoms** of cyber security, through the alliance we could undertake activities such as:

1. Increase promotion of get safe on line through IET/BCS and PEI membership/press office.
2. Help promote CESG 10 steps to cyber security through IET/BCS and PEI membership/press office.
3. Development of a Cyber security health-check for specific sectors.
4. Providing guidance in a phased approach by addressing specific sectors thought to be most vulnerable and that would gain business benefit from such guidance. Advice should be easily understood and practical to apply.

To address the **root causes** of cyber security problems, which is potentially more challenging and longer term, we could initiate workstreams that would focus upon:

1. Help do more via the Trustworthy Software Initiative.
2. Help with proposed legislation such as the draft Consumer rights Bill.

Appended to this document is a position statement summarising the view of the EtF alliance in terms of scope of what is readily referred to cyber space along with steps that may be taken to provide a practical, risk assessed approach to addressing issues around cyber security for various size organisations across differing sectors.

Engineering the Future Position Statement

Key Messages:

1. A single standard for cybersecurity for all users is impossible to achieve and deliver in a way that is meaningful and achievable.
2. The current political orthodoxy is to move away from prescription and bureaucracy so the development of a cyber security "framework" or guidance may be more appropriate.
3. EtF is keen to work in partnership with government to address the issue of cybersecurity and identify potential solutions.

Key issues for consideration

EtF believes that the term cyber security is poorly defined and open to interpretation. This paper sets out to define scope and associated factors that should be considered when addressing issues around cyber security.

1. Scope of cyber security

The suggested definition of Cyber Security as the Confidentiality, Integrity and Availability of data is far too limiting.

EtF defines Cyber as a term that encompasses all forms of communication, monitoring, control, information processing and data storage.

It is particularly important to also include the integrity of automated processes. Threats to the correct operation of software are of major significance (for example, the STUXNET worm). Also 'Data Confidentiality' only partially covers Privacy concerns.

Every one of these elements requires a degree of security ranging from minimum through to high in order to deliver its desired function.

2. Implementation of cyber security on different sectors

Depending upon the type of business environment, cyber security measures and approaches will need to be implemented and managed in differing ways. Some of the different types of sectors include:

Industry
Design, Manufacturing and control systems

Commerce
Banking, Insurance, Travel, Consumer sales, Government departments

Transport
Road, Rail Air, Sea and intermodal.

Energy
Control, monitoring, distribution

All of these sectors will typically employ a range of technologies based on communications and information systems, most of which will rely on a mix of fixed (Wireline) and mobile technology for access. All of these systems rely upon and interact with humans in order to perform some process.

It is for these reasons EtF believes that cyber security cannot be assessed, controlled and managed without taking a holistic view of the operating environment being considered that will in turn dictate the measures and resources required to maintain adequate cyber security in a proportionate manner both in terms of costs and resource.

3. Standards

Standards are an attempt to drive conformity, clarify process and ensure interworking between systems whether, they are physical components, business process or communications systems. All of these attempt to address a vulnerability so as to provide certainty in a particular environment.

However if the standard is not relevant or does not take into account all of the critical processes or components in a system then conformance to a standard does not guarantee the system as a whole will perform as expected.

4. Systematic approach

Every organisation can be considered effectively as a system. Within the system there will be other components that in turn will be sub systems or systems in their own right. In taking a systems approach, then any humans interacting with the system should be considered as part of the system. The human element is particularly important and sometimes the most difficult to predict in terms of behaviour. In practice human actions can often pose the largest risk even if there is no intent.

5. One standard does not fit all

The modern business environment comprises a wide range of organisations ranging from the Micro business through to SME's through to large multinational corporates, all of which operate in a number of differing domains of widely ranging scale and complexity.

At this stage it is import to remember that any cyber related system does not exist in isolation. It exists primarily to support and enable a business or organisational function. For this reason it is vital that cyber issues such as security are considered an integral part of the organisation or system.

Particular standards may be adopted if it is affordable and seen to provide business benefit, for example remediating a threat or perceived vulnerability. However any standard adopted without considering its impact and fit within an organisation is unlikely to provide the safeguards anticipated. It is for these reasons EtF does not believe there is one standard that fits all organisational requirements.

So what is required?

EtF's view is that to focus upon identifying a single standard is the wrong approach and is at odds with the industry definition of standards.

A more appropriate approach would be to consider the development of a framework or an approach along the lines of;

- A Code of Practice for cyber security.
- A Good practice guide to cyber security.
- A cyber security business operating manual.

The guide should take a business process perspective and ensure cyber measures are integral to the organisation functions and management.

If standards are to be adopted to address a particular issue, then ideally they should be internationally recognised so as to be relevant. As businesses operate in ever growing global markets, this will be particularly relevant to UK companies bidding for service provision or the manufacturing of product for export

Special Considerations

In compiling the framework or guide document, consideration needs to be given to the diversity of organisations that exist so as to provide practical guidance that is affordable to implement and balanced against risks. Some of the organisational factors that should be addressed are listed below.

- The size of the organisation, i.e. micro, SME, large, global.
- Customer base – location, sector.
- Sensitivity and criticality of information and communications systems utilised.
- Is the organisation a supplier or user of information and communication systems.
- Does the organisation operate on a global scale.
- Does the organisation have offices or facilities outside of the UK.
- Skills of the employees.
- Senior Executive backing and responsibility Cyber programme and counter measures.
- Is there an existing Quality Management System (QMS) such as ISO 9001, TL 9000, ISO 27000, SOX etc.
- If there are no recognised QMS standards adopted or it is considered too expensive in terms of resourcing, is it feasible to utilise some form of lean process to manage organisational effectiveness.
- Are there any special customer requirements.
- Are there other organisations and expert groups who can help.

Threats and Risks

Overlaying the organisation aspects are the differing levels of threats that will apply to different sectors and types of organisation. These differences will demand equally different approaches to safeguard the cyber environment. One threat hierarchy that might affect a range of organisations is;

- Advanced Persistent Threat (APT) – which also includes State-sponsored espionage.
- Organised Crime.
- Industrial espionage & theft of Intellectual Property.
- Ordinary Crime.
- Hacktivism.
- Threats to Customer Privacy/Personal Information.
- Cyber Vandalism/mindless Hacking.