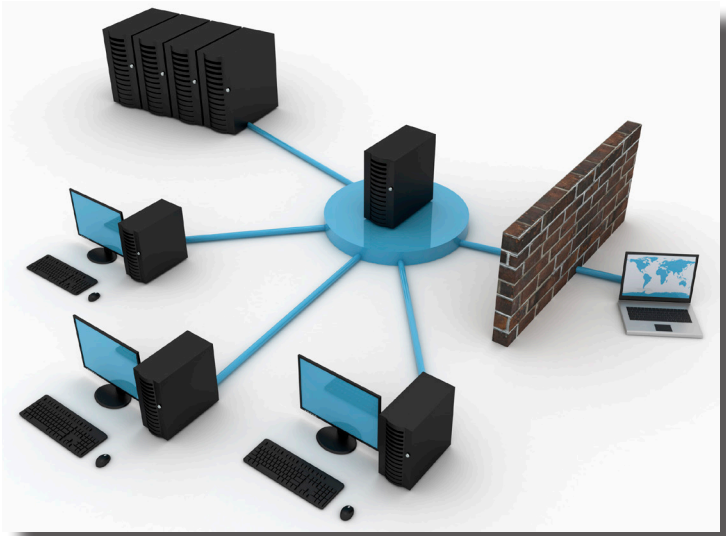
The Institution of Engineering and Technology

http://www.**theiet.org**/cpd

Information Assurance Strategy

A Position Statement provided by the Institution of **Engineering and Technology**



www.theiet.org/factfiles

About This Position Statement

The Institution of Engineering and Technology acts as a voice for the engineering and technology professions by providing independent, reliable and factual information to the public and policy makers. This Position Statement aims to provide an accessible guide to current technologies and scientific facts of interest to the public.

For more Position Statements and Factfiles on engineering and technology topics please visit http://www.theiet.org/factfiles.

The Institution of Engineering and Technology

The Institution of Engineering and Technology (IET) is a global organisation, with over 150,000 members representing a vast range of engineering and technology fields. Our primary aims are to provide a global knowledge network promoting the exchange of ideas and enhance the positive role of science, engineering and technology between business, academia, governments and professional bodies; and to address challenges that face society in the future.

As engineering and technology become increasingly interdisciplinary, global and inclusive, the Institution of Engineering and Technology reflects that progression and welcomes involvement from, and communication between, all sectors of science, engineering and technology.

The Institution of Engineering and Technology is a not for profit organisation, registered as a charity in the UK.

For more information please visit http://www.theiet.org

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no 211014) and Scotland (no SC038698).

Enquiries

policy@theiet.org

Contents

Executive Summary **3**
Independence of the Information Commissioner 3
IA Standards and Delivery Capabilities 3
Educating Society 3

Independence of the Information Commissioner **3**

Information Assurance Standards & Capabilities **3**

Educating Society **4**

End Notes **4**

Executive Summary

Independence of the Information Commissioner

The Commissioner's organisation should be funded separately from the Government of the day and thus be seen to be clearly and unambiguously independent of the Executive.

To reinforce independence, the Commissioner should be appointed directly by Parliament for an extended term of office, say, seven years.

The Information Commissioner should be properly resourced to give good customer service.

IA Standards and Delivery Capabilities

The National IA Strategy recognises the need for stronger IA standards and delivery capabilities, but it does not acknowledge the magnitude of the task and the need for sustained strategic action.

IT systems that protect highly sensitive data (such as health or financial records for millions of citizens) need a level of assurance greater than that required for many safety-critical systems. This is because they need to resist systematic and intelligent probing for possible vulnerabilities.

Very few people have the skills, methods or tools that are essential to develop highly assured software. Those purchasing software have a duty to ensure that those skills are available within the supplier company and that they are employed.

The National IA Strategy needs to recognise this market failure and to take strategic action to ensure that in five or ten years time it will be possible to procure IT systems that can adequately protect highly confidential data (such as the health records or financial data of millions of UK citizens). Until this time, the IA Strategy should state that it would be most unwise to assume that datastores containing large concentrations of confidential data can be securely connected to widely accessed networks without unacceptable (and unquantifiable) security risks.

Educating Society

The benefits of electronic commerce, electronically delivered government services and the social benefits of electronic social interaction will never be realised unless everyone has some basic, jargon free understanding of the core principles of information assurance in the information age. Until Society reaches that state, no amount of job based education will ever prevent the lapses in basic procedure that have been well publicised in recent months.

Independence of the Information Commissioner

The IET proposes that the Commissioner's organisation should be funded directly by Parliament or in some other way that is clearly and unambiguously independent of the Executive. The Commissioner should be a 'people's advocate' and should not remain in the invidious position of always looking over his shoulder with respect to the next year's budget.

At present the Information Commissioner's function is funded partly from government and partly from the fees collected through the data protection registration process. This registration process, of itself, has little point and should be replaced by a requirement for organisations to publish on their websites the details that they are currently required to register.

The Commissioner should be properly resourced to give good customer service rather than running the extensive backlogs of cases as a result of excessive budget constraints. This has sadly become the norm in the 'Freedom of Information' (FOI) area. For example, in March 2007 the ICO had 147 Freedom of Information complaints over nine months old that had not even been assigned to an investigating officer.

To reinforce independence, the Commissioner should be appointed directly by Parliament for, say, a single seven-year term.

Information Assurance Standards & Capabilities

The National IA Strategy recognises the need for stronger IA standards and delivery capabilities, but it does not acknowledge the magnitude of the task and the need for sustained strategic action.

Making IT systems secure is a greater technical challenge than making them safe. This is because security-critical systems have to resist systematic and intelligent probing for possible vulnerabilities whereas most safety-critical systems only fail because the conditions that trigger failure occur by chance during their operation, IT systems that protect highly sensitive data (such as health or financial records for millions of citizens) therefore need a level of assurance greater than that required for many safety-critical systems.

It is widely understood by computer scientists and software engineers that testing software is a wholly inadequate way to establish high reliability. In particular, testing is almost useless as a way of showing that software does not contain the sort of obscure errors that lead to breaches of security. (This is an inescapable consequence of the nature of digital systems, which may exist in billions of logically different states).

Unfortunately, very few systems companies (and even fewer in-house software teams) have the skills, methods or tools that are essential to develop highly assured software. As a consequence, any systems that are built from commercial off-the-shelf (COTS) products are highly likely to be insecure (and certainly cannot be shown to be secure).

A recent study for the US National Academy of Sciences[1] concludes that there is a need for stronger software engineering methods, which are soundly based on computer science and mathematically rigorous. Such methods do exist and they have been shown to be practical and cost-effective[2] but the methods are not yet widely adopted by software developers.

The National IA Strategy needs to recognise this market failure and to take strategic action to ensure that in five or ten years time it will be possible to procure IT systems that can adequately protect highly confidential data (such as the health records or financial data of millions of UK citizens). Until this time, the IA Strategy should state that it would be most unwise to assume that databases containing highly confidential data can be securely connected to the internet without unacceptable (and unquantifiable) security risks.

Educating Society

Security of personal and confidential information within the domain of computer systems has become a critical issue for all. Recent losses of personal data and the rise in identity fraud attract a large share of journalistic attention and we are bombarded with advice from every quarter. But most of what we read, beyond a superficial level, contains incomprehensible technical detail and impractical recommendations.

Before computer use became the norm, information assurance was simply a matter of managing filing cabinets and the documents within them. The words 'Confidential' or 'Secret', 'Do not Copy', 'For xxx's eyes only' make intuitive sense to us all. Information was assured by the using trained personnel, rigorous lock and key management and the ultimate threat of dismissal or even criminal proceedings.

A physical intrusion into a locked cabinet is quickly detectable. However an electronic intrusion may go undetected for ever. Today, the complexity of computer security techniques has led to the state where only a handful of technical specialists have even the remotest idea how to handle the computer equivalent of the locked filing cabinet.

The recently reported breaches of information security of personal information within both public and private sectors demonstrate well this lack of basic awareness and understanding. Not only were the procedures inadequate but also the volume of exchanged information was inappropriate.

The CSIA Information Assurance Governance Framework, published on 22 November 2007 discusses awareness, education and training on pages 37-38. It is aimed at "the general population of users" with an implied tacit assumption that those users are within the civil service and its subcontractors. It correctly identifies the need for 100% coverage of basic education for the whole of this population, not just IT staff. It stresses the need for the establishment of a security culture rather than just providing information. It insists that programmes must include refresher courses to be effective.

Such awareness and education must not be seen to be the preserve of the civil service alone. It must extend to all employees in all sectors and to their families. Embedding an information assurance culture needs to be started in our schools and colleges well before employment age.

We need to approach, very rapidly, the state where society is as familiar with the risks arising from careless handling of electronic information as it is with paper based equivalents. We need to be able to react intuitively to issues and problems as they arise and to know when our actions are likely to tip us into a risky situation.

Until everyone has some basic understanding of the core principles of information assurance in this information age, the huge benefits of electronic commerce, electronically delivered government services and electronic social interaction will not be realised.

End Notes

1. Software for Dependable Systems: Sufficient Evidence? http://sites.nationalacademies.org/cstb/completedprojects/cstb_042247
2. The US National Security Agency carried out a recent experiment that showed this.

The Institution of Engineering and Technology

The Institution of Engineering & Technology
Michael Faraday House
Six Hills Way
Stevenage
SG1 2AY

01438 765690 - Policy Department
email: policy@theiet.org
http://www.theiet.org/policy
http://www.theiet.org/factfiles

This content can contribute towards your Continuing Professional Development (CPD) as part of the IET's CPD Monitoring Scheme.
http://www.**theiet.org**/cpd