Accreditation: An end-to-end approach to managing information assurance within the Ministry of Defence

Underpinning modern information systems with effective information assurance is by no means a simple task. **Paul Shanes** and **Dr. Chez Ciechanowicz** explain how to ensure an information system is appropriately secured and fit for purpose.

The rapid advancement and widespread growth of information technology has led to organisations becoming increasingly reliant upon complex information systems to underpin their core business processes. This paradigmatic shift has been seen as a major opportunity to integrate services across the public sector, with government departments keen to leverage the benefits that ever enhancing technology can provide when delivering essential goods and services to their citizens.

Recent exposure of government departments that have fallen victim to attacks against the information they process means that public awareness of the dangers inherent to the electronic processing of data has never been so high. As a direct consequence both ministers and senior civil servants are becoming increasingly aware of the need to maintain effective information assurance in order to engender trust amongst their citizens, while delivering personalised public sector services in a secure and effective manner.

Underpinning modern information systems with effective information assurance is by no means a simple task. Technology within the workplace is still very much in its infancy. This is particularly true within the public sector which little over a century ago, in 1885 purchased its first ever typewriter much to the protest of calligraphers within the Civil Service. In the early 1900s the Civil Service made another bold move with the introduction of telephones across central departments.

Clearly much has changed throughout the last century with public sector spending on Information and Communication Technologies (ICT) averaging some £16 billion pounds every year[1]. Technological advances continue to enhance healthcare, defence, safety, security and the education system, but with technological advances revolutionising the lives of citizens across the world the role of safeguarding state of art and sometimes 'bleeding edge' technology is continuing to prove extremely difficult.

The methodology implemented across the public sector to ensure an information system is appropriately secured and fit for purpose is known as accreditation. The government defines accreditation as "the formal assessment of the information system against its information assurance requirements, resulting in the acceptance of residual risks in the context of the business requirement[2]."

The Central Sponsor for Information Assurance (CSIA) was established within the public sector in

2003. Headed initially by the Cabinet Office and subsequently by Government Communication Headquarters (GCHQ) "the CSIA aims to assure government that the risks to the information systems that underpin key public interests are appropriately managed[3]." CSIA further defines the concept of information assurance as confidence that information system's will "protect the information they handle[3]," to ensure confidentiality across the system with the confidence that operation of key assets will not pose an unacceptable risk to the host department, "function as they need to, when they need to[3]," to ensure integrity and availability across the system and "be under the control of legitimate users[3]," to ensure authentication and non-repudiation across the system.

The application of appropriate information assurance grounded by an accreditation process enables businesses and government organisations alike to exploit opportunities which would previously have been considered too great a risk. As such, any decision to accredit an information system is best made with the full understanding of any business requirements and limitations, as it is the business itself which must live with a compromise, be it accidental or deliberate for any of the risks which materialise.

STANDARDISED RISK MANAGMENT AND DEFENCE-IN-DEPTH

Within the MOD a standardised risk management methodology exists for the accreditation of information systems. The fundamental basis of this accreditation process relies heavily upon the notion of 'defence-in-depth.' This notion is where a number of countermeasures or controls are employed in order to mitigate a specific risk, or set of risks and thus reduce the residual risk to an acceptable level. The defence-in-depth initiative can employ a variety of controls from different

The application of appropriate information assurance grounded by an accreditation process enables businesses and government organisations alike to exploit opportunities which would previously have been considered too great a risk.

security facets to achieve the desired result, for example an infrastructure may be protected against technical attack by an evaluated and appropriately configured firewall and intrusion detection system (technical controls). The results of these can then be monitored (procedural controls) and reported upon by appropriately cleared personnel (personnel controls).

In order to determine the importance of the defence-in-depth approach, we can consider the philosophies of soft systems methodology, in particular Checkland's notion of emergent properties which states "properties which refer to the whole are meaningless in terms of the parts which make up the whole" and more importantly that "the whole is more than the sum of its parts[4]." When interpreted in relation to information assurance we can determine that while useful in a given context, a particular security control will be much more effective when employed as part of an overall model of security controls. For example the fence protecting a site is much more effective if monitored by closed-circuit television system and security guards. It is this logical combination of controls which enable the MOD to gain assurance that information is being appropriately safeguarded.

The defence-in-depth approach coupled with a robust accreditation process enables the MOD to accurately quantify information risk in a logical and thorough way. This has enabled a cultural shift, from a department which historically has been extremely risk-averse to one which is able to adopt a methodology of risk management, enabling it to make better use of technology and provide improved services to the armed forces.

The difficulty however, emerges as government information systems continue to become more widely inter-connected, making use of modern day, untrusted technologies and communication media, such as those afforded by cyber space. For this reason a suitable methodology is not only required by the MOD but more widely by a multitude of government departments, if they are to follow a consistent risk management approach which will enable them to operate collaboratively in the future.

ACCREDITATION AND REAL-TIME DATA EXCHANGES

In order to realise the vision of joined-up shared services across the government, departments must first understand the environment in which modern information systems now operate. Proliferation of networks and the advent of 'cyber

space' are changing the very nature of interaction between governments and their citizens. If the public sector is to keep up with this unprecedented period of change, the departments too must continue to develop means of interacting with citizens in the way in which they have become accustomed. As a result, information sharing requirements now exist across a multitude of departments.

It is clear that technological advances in networking and the proliferation of the Internet pose a new and very real element of risk to modern government networks.

In order to facilitate near real-time exchanges of data, the vast majority of information retained by the government must be stored in electronic form. Consequently, many key services have now made traditional paper-based records obsolete, placing almost complete reliance on vast and complex electronic infrastructures to support their core business requirements.

It is clear that technological advances in networking and the proliferation of the Internet pose a new and very real element of risk to modern government networks. The relatively low cost and anonymity of the Internet makes it an ideal attack vector for criminals, foreign intelligence services and terrorists alike. As such it is essential that the risks to public-sector information systems are appropriately assessed, managed and monitored in line with other business risks.

Although accreditation is widely accepted as being necessary, and historically has proven to be a very effective method of managing information risk, the changes in operating environment and increasing expectations of citizens requires the various public sector organisations to agree upon a consistent framework of methodologies by which to quantify and manage information risk. With each department traditionally being held responsible for their own information assurance, it is no surprise that conflicting policies and standards have emerged throughout the sector.

Although government-wide policy and standards exist, they are the subject of much criticism. The Manual of Protective Security (MPS), (government's own version of an Information Security Management System), is complex and burdensome. The document was originally designed for the Cold War era and was last

updated in 1994. Its content relates primarily to the threats of its time, focusing upon physical and procedural security. Amendments which have been made to incorporate technical security measures have resulted in the document continually growing to nearly two thousand pages in length.

Constantly criticised for its complexity and outdated information, the document also suffers from vague content resulting in individual departments interpreting policy in their own way. As a result the document has not been formally adopted by a number of major government departments. The NHS for example has opted to develop its own Information Security Framework incorporating good practice guides, codes of practice and toolkits relevant to the health sector. Likewise the MOD uses its own Joint Service Publication (JSP) 440 – The Defence Manual of Security to govern information security policy.

The information contained within JSP 440 originated out of the MPS, but has since grown to incorporate the specific requirements for protecting military assets, particularly in hostile environments. The policy contained within the MPS has only recently been reviewed and released as the new Security Policy Framework (SPF). Although efforts are being made within the MOD and NHS to align their policies with the new SPF, there is at present no indication that the SPF will replace either the MOD or NHS publications, resulting once again in differing standards. While there are obvious benefits to local variations on security policies, based upon the structure and purpose of particular departments, the same underpinning baseline guidance could dramatically improve understanding across departments aiming to link up and offer truly joined up public sector services.

The general public is constantly being told, particularly with regards to criminal and terrorist activities, that many offenders and extremists could have been detected sooner if departments had communicated and pooled their efforts and intelligence into a single resource. The same argument can obviously be made for the protection of our public sector services and critical national infrastructures. For several years ministers have acknowledged that there are too many disparate areas of government actively involved in information assurance initiatives to focus adequately upon key areas of concern.

Although some would argue that the diversity of multiple departments strengthens the various initiatives, the Conservative Party (when still in opposition), proposed an alternative approach

where the relevant areas of government were linked together to coordinate efforts and expertise under the direction of a single reporting chain. The Conservative Party's approach also acknowledges that the threats faced today through cyber space are equally as complex and potentially as damaging as those related to terrorism, a view shared by the Obama-Biden administration in the United States.

THE UNIFIED SECURITY APPROACH TO INFORMATION ASSURANCE

In the uncertain environment we find ourselves in, it is difficult to determine whether information-related attacks originated from naive script kiddies, with too much time on their hands, foreign governments seeking state information or even extremists intent on causing physical damage to a nation through their destructive actions. The unified security approach proposed by the Conservative Party should go some way towards breaking down the individual barriers which currently exist across government, enabling a holistic approach to information assurance.

Such an approach is desperately needed in order to respond to ever-reducing citizen confidence in the government's ability to manage information assets. Political parties in particular are acutely aware of the tremendous damage that can result, not only to public sector organisations but more importantly their own political party, and as such have very little appetite for reputational impacts resulting from failures to adequately address information assurance requirements.

The unified security approach proposed by the Conservative Party should go some way towards breaking down the individual barriers which currently exist across government, enabling a holistic approach to information assurance.

As such it is now commonplace for one to consider the prospective damage to reputation as being equally or even more important than the more traditionally recognised confidentiality, integrity and availability concerns. It is this reducing appetite, together with public intolerance of negligence on the part of government organisa-

tions, which has led to a plethora of legislation surrounding the disclosure of information and appropriate operation of communications and information systems.

Government organisations must tread extremely carefully to determine the appropriate balance between implementing effective security which satisfies the rights of their citizens, while not infringing the rights of their own employees by overzealously or unnecessarily monitoring their activities. As a direct result of recent losses and growing concern over reputational impacts, the government has determined that a higher level of maturity is required in information risk management.

Assurance is now required over and above minimum baseline requirements in order to ensure that government departments adhere to best practice measures and standards in line with their industry partners. This is essential, not only to prevent high profile data losses and the reputational damage that results, but more importantly because modern citizens have begun to build up a perception of what to expect from secure online services, due to increasing online interaction throughout their day-to-day lives.

It is easy to underestimate the difficulty of improving the level of information assurance across an organisation, particularly one within the public sector. In an attempt to embrace government strategies and initiatives many organisations have found that simply delivering an improved ICT system or infrastructure has been insufficient to realise desired business benefits.

The UK is not alone in its efforts to improve information assurance across public sector services, with many other developed nations experiencing similar difficulties, including the US. The Obama-Biden administration has acknowledged that a thorough review of information assurance across the federal government is required and, although elements of the US government significantly disagree upon the nature and magnitude of the threats faced, there is agreement that the threats are in fact very real, and very difficult to counter.

This can be likened to the change in political direction within the UK where the Conservative Party is reviewing the approach to information assurance across the public sector. Comparative analysis shows that the US and UK are both striving to achieve very similar goals when exploiting the opportunities which cyber space can offer, but both suffer from similar issues, centred around the difficulty in implementing cohesive and standardised policies and procedures.

It is only with bold moves, such as the formation of end-to-end chain of commands with ability to reach the senior most levels within government and national awareness campaigns to improve awareness throughout the entire population, that countries can adequately address information assurance. Furthermore it is clear that 'like-minded' developed nations such as the US and UK should collaborate in order to face new challenges which will clearly affect us all.

CONCLUSION

In the words of US Secretary of State Hillary Clinton: "In an Internet-connected world, an attack on one nation's networks can be an attack on all[5]." This notion alongside acknowledgement that cooperation and collaboration is required both domestically, as well as with 'like minded nations' further emphasises the view that "we are stronger and more effective when we work together than apart[6]." This realisation is essential in order to address the threats emerging through the use of modern technologies and communications media such as those afforded by cyber space.

The true test will be whether countries such as the US and UK can work together to lead other western world nations in a unified approach to addressing such challenges, in order to win what appears to be a modern 'arms race' in cyber security. This, coupled with standardised policy and processes, supporting joined-up shared services across governments can only build upon the already strong processes of accreditation within individual departments such as the MOD and work towards enhancing the overall maturity of information assurance across the wider public sector. ■

ABOUT THE AUTHORS

Paul Shanes joined the Ministry of Defence after graduating from university and opted to pursue a career in information security. Whilst studying for his MSc in Information Security at Royal Holloway, he was employed as a Security Accreditor for the Defence Security Standards Organisation. Having gained his MSc, he is now employed as a Senior Security Assurance Manager, advising departments on security and data protection matters.

Dr. Chez Ciechanowicz is a Reader in Information Security.

FOOTNOTES

1 Cabinet Office, Government Information Communication Technology Strategy (Smarter, Cheaper, Greener), *Her Majesty's Government*, December 2009

2 National Infrastructure Security Coordination Centre, Risk Management and Accreditation of Information Systems, *Her Majesty's Government*, August 2005

3 Cabinet Office, Coleman, N, Protecting Government Information (Independent Review of Government Information Assurance, The Coleman Report), *Her Majesty's Government*, June 2008

4 Checkland, P and Scholes, J, *Soft Systems Methodology in Action*, Wiley & Sons, 1990

5 Harvey, M, Hillary Clinton Guards Internet Freedom In Attack On China's New 'Berlin Wall,' *The Times*, 22 January 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/article6996738.ece

6 Cabinet Office, Transformational Government (Enabled by Technology), *Her Majesty's Government*, November 2005