



Human Vulnerabilities in Network Security

Summary

In order to strengthen network security there is a need to address human, as well as technological, vulnerabilities. Human vulnerabilities in network security may arise inadvertently, due to a lack of understanding of security by the network user, or deliberately, due to insider fraud. In particular, there is a need for organisations to establish effective security cultures and to assess the potential risks that are posed by their employees.

This collaborative research & development competition provides a challenge and an opportunity for UK industry and academia to deliver innovative and sustainable long-term solutions to realising these goals.

To support business in meeting these aims, an indicative amount of £1m has been allocated in this competition to support projects that address the challenge of establishing effective security cultures and employee risk assessment. **This is a 'challenge-driven' approach that we are piloting for the November 2006 Competition, encouraging consortia to focus on achieving solutions to a societal challenge.** Support will be in two stages – initially through supporting short feasibility studies, the best of which will be selected, leading to longer-term collaborative research and development projects, with the ability to make significant change.

Network Security Innovation Platform

Innovation Platforms (IP's) are a new way of working for Government and business, developed by the Technology Strategy Board and should be seen as an opportunity to position business and government closer together to generate more innovative solutions to major policy challenges. They are designed to address a challenge, bring together Government stakeholders and funders, and engage with business and the research community to identify appropriate action. They should create a win-win situation, with government getting more innovative solutions at reduced risk, and UK business well positioned to win major UK and global competitive procurement opportunities, by bringing together a range of technologies and policy levers to deliver innovative new products and services for which there are real customers in a potentially large global market.

Background

The weakest link in network security is not usually a technological vulnerability but the people that work with systems. To give a simple example, the most secure system can be easily penetrated if staff that have legitimate access write down their password or let it be used by someone else. Security can be compromised either accidentally because there is a lack of perception or realisation of security or deliberately for illegitimate purposes such as fraud.

In order to address the human vulnerabilities in network security, organisations need to create working environments that discourage negative behaviour and which make it hard for such behaviour to go unnoticed. They also require analytical tools for assessing the level of risk posed by their employees. These two approaches – one focussing on the individual

and the other focussing on the organisational culture – would be complementary components of an effective security regime.

Scope for Applications

1. Establishing effective security cultures

An effective security culture is one that reduces personnel security vulnerabilities (i.e. the potential for staff to abuse their access to the organisations assets). What does this actually involve: what social structures, rules and attitudes should exist in an effective security culture? How is it possible to create and embed these cultural characteristics in an organisation? And how should an organization determine whether it has managed to create those characteristics – how do you measure security culture and with what tools?

For many businesses to enhance innovation, motivation and thus performance, employees confident in and extending capabilities of networked systems can be important for improved performance but pose new risks to network security. How can business best manage this paradox between capabilities and vulnerabilities?

2. Employee risk assessment

To what extent is it possible to assess the risk that an employee will abuse their access to an organisation's assets for illegitimate purposes (e.g. abuse their computer network access). These assessments should take account of the opportunity afforded the employee by virtue of their access to the organisation's assets. They should also take into account any anomalous patterns of employee behaviour. In practice, how should such risk assessments be done? What assessment processes can be used to combine the elements of risk in a practical method? What methods and tools can be used to analyse records of employee activity in order to detect anomalous patterns?

In both cases, the aim is to draw on technological and social science research to develop approaches and practical tools that can be used by organisations to enhance their security.

Project Details

Support is planned to be delivered in two stages – short feasibility studies (to be selected through a one stage process), which once completed, will be assessed and the best (those demonstrating an ability to make significant change) may be selected for longer-term collaborative R&D projects. At this stage we are only seeking feasibility studies (science to business and business to business) which take less than 6 months to complete and are expecting between £50k and £100k of Government funding.

The studies supported will aim to establish the feasibility of a particular idea, thus forming the case for support of the subsequent, if selected, longer-term collaborative research and development project. The feasibility study should aim to deliver the following:

- summary of the technological, and socio-technical innovation;
- summary of the economic, environmental and societal benefits;
- supply chain impacts;
- detailed plan for further research and development, trialling and for delivering project benefits and diffusion.

The feasibility studies, once completed, will be assessed as part of a competitive process. Those assessed to be capable of delivering the best overall benefits will receive Government support of up to £1m to undertake longer-term collaborative research and development projects. These could include large-scale integrated projects. The projects supported will be expected to bring

together all the required resources and activities to deliver significant change, delivering innovative methods of effective communication of security to the non specialist user and new systems and environmental design to reduce insider fraud. Projects will generally aim to implement significant business change in a 5-7 year time frame, rather than offer immediate payback. Support will be particularly focused on solutions that can demonstrate generic applications.

Other Funding Opportunities

The Economic and Social Research Council will be making available in the region of £500,000 for dual research applications at both stages, which must have business engagement. There may also be opportunities for Research Council co-funding of particularly novel projects at the feasibility stage and for longer-term projects. Applicants may also independently seek to bring in other sources of public funding for the longer-term projects where appropriate for example, Regional Development Agencies, Devolved Administrations or other government departments. Note that total public funding for each project cannot exceed the limits indicated in the 'Guidance for Applicants'.

Contact

If you have any queries about this technology area please contact Jessica Rushworth at the DTI.

Jessica.rushworth@dti.gsi.gov.uk

020 7215 1718

For information about the application process please visit

<http://www.technologyprogramme.org.uk/>

This website contains guidance for applicants, including deadlines and dates of applicant briefing sessions.

Alternatively call the helpline on **01355 272155** or email info@technologyprogramme.org.uk