Lock down or open up?

Utilities face a dilemma: keep IT security tight and restrict useful information flow, or share information and risk attack. Tim Arridge and Peter Franklin seek lessons from the military

We all now live in the shadow of potential cyber attack. Information security and assurance have become priorities for all organisations, but none more so than those responsible for critical national infrastructure. Many utilities have retreated behind firewalls to protect themselves. The priority of their IT departments is to minimise the possibility of incursion at all costs, by isolating their systems from the external world.

However, the need to protect information should be balanced against the need to share information in a controlled manner. Insufficient attention to information security can lead to disaster, but too much or incorrectly configured information security can choke business-critical information flow. In utilities, this could have major consequences for both network capital expenditure and operating costs, and supply business trading and balancing costs.

This is a fact today but will become truly serious as we move into a smart grid world. There the integrity of networks will be dependent on electronic interconnections with countless devices external to the organisation – for example, in the context of demand response. With utilities facing expenditures in excess of £100 billion over the next 20 years, getting the balance right will be worth tens or hundreds of million of pounds, and possibly billions.

The military sector leads the field in secure systems and has made huge investments in research and development. Modern warfare requires both the highest levels of security and effective real-time collaboration between land, sea and air forces, intelligence groups and often troops drawn from multiple countries. There is much that the energy industry can learn from this experience.

The best way to achieve the right balance between security and connectivity is to undertake a systemic, military-grade assessment of connectivity benefit versus security risk. The first step is to detail all the issues in play and how they interact to create or destroy value for the enterprise, explicitly extracting input from all important stakeholders inside and outside the organisation. This will ensure all relevant factors are taken into account.

Next, all risks, costs and benefits should be translated into a standard measure of value in pounds sterling. This allows alternatives to be weighed up in common terms in a technical, logical and commercial manner. This is not straightforward, and hard questions have to be asked. But only by calculating the monetary value of alternatives can trade-offs to be rationally debated and selected.

Utilities may even want to consider working with military experts in the field to ensure they get the security and connectivity balance right. Military precision would be a valuable attribute for a smart utility.

Tim Arridge is an information risk specialist at Frazer-Nash and Peter Franklin a utilities specialist at Enstra Consulting