NATIONAL INFRASTRUCTURE DEPENDS ON STANDARDS

Stephen Munden considers the unique role that standards and assurance can play in securing CNI and other valuable assets

In the context of security management, standards can identify critical components of the security management system, performance criteria and their relationship with other components. In other words, form, function and fit can be described within an integrated and multi-layered environment, such as security, by using standards.

In fact, whether it is realised or not, all successful businesses are underpinned by a network of connected standards, which can define anything from the organisation's brand, technology and values. It is also true that management sets the standards for the entire organisation when it communicates its business plan.

This approach has been used effectively for some time by quality practitioners implementing ISO 9001-compliant management systems. Within an organisation's value chain, standards have been used to highlight where the value lies and eliminate activities and assets where they do not. Compliance against standards can then be quantitatively or qualitatively measured and a degree of assurance gained about likely performance outcomes.

A few years ago Business Keys was commissioned by the Perimeter Security Suppliers Association (PSSA) to develop a Product Verification Scheme. The idea behind the scheme was to raise standards within the perimeter security supply industry and gain some confidence that the product being supplied was the same as that put through earlier impact testing. Impact testing being one on the key performance criteria for physical vehicle security barrier systems (VSBs), such as blockers, gates and bollards.

When we looked at the standards landscape, we found that there were not adequate formal standards for perimeter security barriers, fences, or indeed their installation. CPNI had led the way by developing, through BSI, a Publically Available Specification (PAS 68 – now ISO IWA 14) for impact testing but other safety, environmental, operational and security criteria were not adequately defined. And so the first job was to gain industry consensus around specifications for VSBs, high

©Getty Images

The sound advice given by security advisors may be compromised if the advisor is not invited back to confirm that the advice has been correctly applied

security fencing and their installation.

All we would have to do then, we thought, is verify that the supplier had an accredited ISO 9001 quality management system, the product was safe (i.e. it met the Essential Requirements contained in EU product safety directives), and there was evidence of a valid (PAS 68) impact test.

What we have found in practice over a number of years of implementing the Verification Scheme is lots of well-meant activity but very little assurance of security being achieved. There appear to be a number of factors contributing to this situation.

Firstly, the lack of agreed criteria in formal and informal standards, notwithstanding the need to keep some information restricted because of the nature of security, is adversely impacting the specification and so procurement of perimeter security equipment.

Secondly, current security assurance mechanisms are not fit for purpose – see box out for more on this. And thirdly, as if it wasn't bad enough that current standards, specifications and conformity assessment mechanisms are complex, inefficient and deficient, the industry itself is still relatively immature and its supply chains fragmented.

Supply chain fragmentation is particularly concerning. We have seen examples where suppliers, often with vast experience and knowledge, have not had reasonable access to site requirements, resulting in inappropriate security solutions being installed. From the other end of the supply chain, the sound advice given by security advisors may be compromised if the advisor is not invited back to confirm that the advice has been taken. And in the middle can be a range of organisations hell-bent on price reduction, often at the expense of security. The security solution becomes a construction commodity, which may not serve its purpose either when called upon in a life-threatening emergency, such as a terrorist attack, or because the product design will simply not afford the protection sought in the site-specific circumstances.

Given these institutional and commercial barriers, how can the practising security professional overcome what seem to be insurmountable barriers, beyond the control of an individual organisation? As eminent scientist Stephen Hawking has pointed out, "We live in a universe governed by rational laws that we can discover and understand" and therefore "make informed decisions". Those laws apply to all of us, whether we understand them or not. In the same way, international and national laws apply to security products and security practice. Standards, which are simply an agreed way of doing something as opposed to a mandatory requirement can be used in a similar but much more agile way.

Continuing with the example of perimeter security, our task regarding standards was to find a way of addressing the challenge that ALL relevant standards could be verified, not just one by one and not separately. To successfully apply standards and assurance to security (and some have now adopted the phrase "organisational resilience"), we had to adopt a new paradigm.

Since we didn't have large resources and the time for formal standardisation, we developed our own specifications with the help of stakeholders, including industry representatives and with the help of the security services. Industry, or perhaps more accurately, market standards are often more effective when technology is changing rapidly and a cheaper and more agile approach is required. It should be noted that many of the most successful standards never go through formal standards institutions. The downside of this approach can be that adoption is harder because without the mandate of law or other significant drivers, those who do not understand the initiative often shun it at first.

However, in the case of perimeter security verification, we have specifications in place that address the key areas of security, operations, health and safety and environment, including acceptable criteria that permit verification. By looking at security systemically we have tried to ensure that products and services that PSSA members have had verified will conform to their declared specifications; will represent reasonable security solutions for the specific site and will meet the specified Operational Requirements, as part of the organisation's security risk

NATIONAL INFRASTRUCTURE DEPENDS ON STANDARDS

management system.

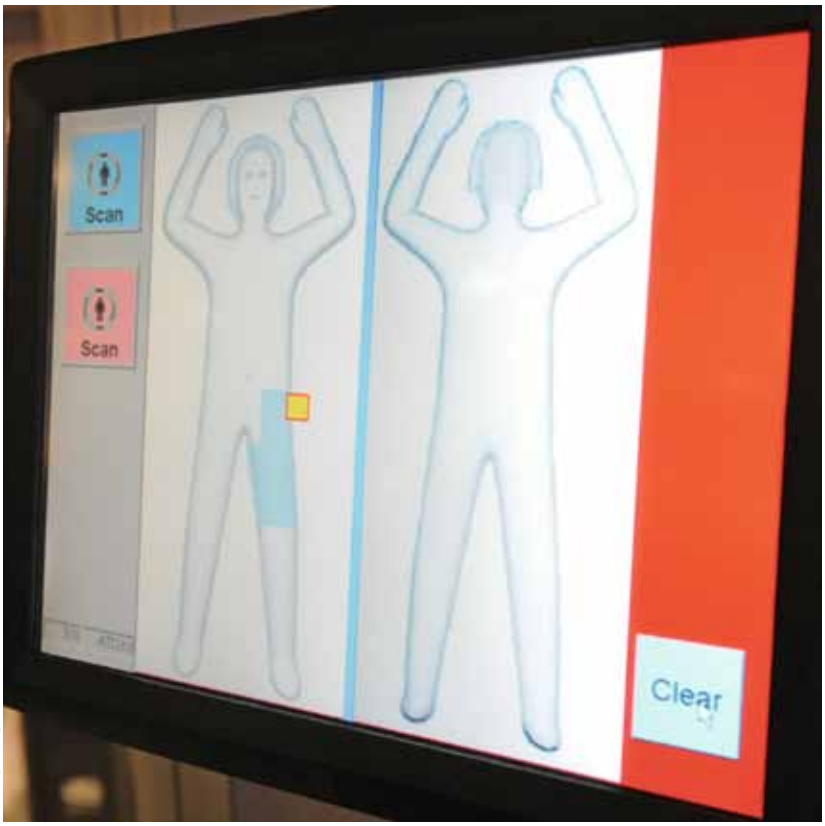
Similarly, when considering verification, we had to look at the contributions to security system assurance that existing 'conformity assessment' mechanisms and alike were making. As explained above, although many users, buyers and specifiers currently rely on the assurance of procuring a "PAS 68 gate from a certified ISO 9001 and many health and safety badged" supplier, this in no way ensures that the security or other criteria for the product have been fulfilled. Nor does it give confidence that the equipment system will be fit for purpose or installed to provide the intended security solution. The trick, therefore, is to leverage the architecture of standards within the supplier's system, as part of the standards within the site system, as part of the security management system of the organisation. In other words, take the simple laws associated with standards and systems to create a more robust assurance paradigm.

So what? The industry needs to wise up to the value of standards in CNI.

There are several learning points from this example that can be used by security professionals grappling with the complexity of international security threats, requirements, legal regimes, user needs and so forth. Standards are not just a set of stuffy technical documents that can be left to 'old George' to take care of while management takes care of business. They are commercial leverage points in a business system that can be used to define, deliver and create value, whether that be in commercial or security terms. Their effective use is only possible if they are deployed at strategic, tactical and operational levels, to do their respective jobs.

Standards are the nodes of the system. They define components, their performance and interrelationship with other parts of the system. Systems have 'laws' relating to their relationships, holistic and emergent properties (such as resilience) and so on. Security systems obey these laws, whether they are understood or not. Assurance can similarly only be gained by addressing systems, in addition to processes, activities and requirements. Point solutions for assessments and audits will not suffice. The individual components alone do not in themselves make up a system.

The points that I have tried make here, of course, imply that security itself must be managed within the wider systems context. Indeed the 'laws' apply to the organisation itself. Some may have noted the introduction of ISO 9001: 2015 and other ISO management standards being developed to a similar list of contents, which lean towards 'integration' of management systems. (Impossible, since they can never be dis-integrated – everything is connected to everything else). The wise security practitioner will focus not so much on the advertised gains in being able to use less documentation or do less auditing, but more on how their security management system, health and safety management system, environmental management system, *etc.* themselves work in harmony to address issues such as protection of people, emergency evacuation, optimum efficiency and so forth.



©Getty Images

A scanner such as the L3 ProVision Body Scanner can help to provide a more joined-up approach to security

Current problems with security assurance

- Certification to ISO 9001 by certification bodies addresses processes and customer satisfaction – not product quality (hence the saying that a company can be certified, but can consistently produce rubbish).
- The current processes of accredited certification call for certification against a specific standard, but businesses operate as systems AND products are in fact systems, meaning that security must also be managed as a system.
- Suppliers, often SME's, are forced by government departments and larger customers to gain multiple certifications to a plethora of (mainly health and safety related) standards and schemes, all underpinning the same regulations and many claiming to be 'one-stop shops'.
- A recent addition to the Pre-Qualification Questionnaire problem, which is similar to the health and safety compliance chaos but broader, is the appearance of multiple supply chain assurance mechanisms and accompanying lists, which a supplier must be on to do business.
- Users/buyers/specifiers do not ask for – and some less reputable suppliers do not have – robust inspection and test plans providing evidence of conformity to appropriate standards.

Stephen Munden is Director of international management systems at compliance specialists Business Keys Ltd.