Standardising global security

Controlling identified risks at all of your sites, anywhere in the world, can be difficult. Especially when taking budget constraints into account. How can you ensure all of your people have a secure working environment? And that all employees, everywhere, adhere to your security policy? Standardising security gives this assurance and more. It not only minimises risk and guarantees compliance, it reduces operational requirements too. So maintenance costs for your entire physical security solution are minimised. Despite this, global standardisation isn't common business practice in security yet, even though it's widespread in other industries. So what can we learn from these industries when implementing a global solution for security?

by Nancy Wanders

Inspiration from the IT world

Given the benefits standardisation offers to international enterprises, it's clear why the need for a global security solution is rising. In contrast to other fields such as IT, however, multinationals tend to have little experience in globalising security. As it involves a large project spanning many years and involving many stakeholders, it demands a high level of project management. In the absence of a structured program with defined guidelines, a global security rollout is likely to be a stressful execution. And one where staying on time and budget is a challenge. The big benefit we have in our industry, though, is that we have the opportunity to learn from the global rollout of IT solutions, so we know what clients need during projects on this scale.

A tried & tested approach

Maintaining transparency on project status is key during large-scale, complex rollouts. Although difficult to achieve, it's necessary to stay fully in control and constantly up-to-date on the entire programme. Project management methodologies developed for other industries, such as PRINCE and IPMA, are tried and tested in guiding, aligning and controlling global projects. We can take the best practices from these and work them into a delivery framework for clients implementing global security. Only by applying a robust delivery framework can we ensure the defined quality standards are met, and all local projects are delivered on time and within budget.

A global rollout involves many different, local implementations and a wide variety of factors. So, as well-established project management methodologies have taught us, it's important to divide the rollout into many smaller, more manageable projects or phases. To keep track of progress and manage the whole programme effectively, each separate phase and the related tasks and responsibilities need to be defined. And, more importantly, they need to be documented. Each phase must then be signed off before the project can be taken to the next phase.

This provides a transparent structure for the entire process. All stakeholders within the programme remain updated on status, deliverables and milestones enabling the programme's progress to be monitored and steered.

Best practice methodology for security

The first phase of a global rollout programme involves establishing and documenting requirements. A high-level plan, covering the different tasks and responsibilities involved in the programme, can then be drawn up. This is followed by detailed planning to define the approach for every element of the project.

Once this is signed off, the programme is taken into the build phase, which involves establishing central servers and applications. During the pilot phase, the chosen physical security solution is implemented and tested thoroughly on one or more pilot sites.

Models and templates from IT best practices are used to guide and align the rollout process, and ensure uniform execution according to determined standards. For example, standardised reporting, providing both strategic and detailed project information, is essential to ensure the programme and individual projects are well-managed and completed on time and to budget.

Quality of implementation enhances quality of technology

When standardising globalising security, the quality of delivery determines the quality of the system. At each local site, good project management and implementation are critical to maximise investments in technology. For security to be successfully standardised, IT best practice methodologies must be applied properly, and tasks, responsibilities and processes defined and documented. Only then can a truly global security policy be established and upheld by unified processes and procedures.