

The ever-changing world of security?

Threats such as Mifare hacking, the General Data Protection regulation coming in 2016, and the need for security to integrate with other IT-based systems – these are just some of the challenges security manufacturers and system users have to deal with and respond to. External factors such as these do provoke change in physical security systems, but it's reactive change. Whereas, in the IT world, innovation and product development occur quickly and proactively. So why do manufacturers of physical security systems have a more reactive attitude towards the changing world? Why does it take external pressure to bring about innovation?



Design for change

The physical security industry doesn't seem to have caught up with the idea that systems should be developed to meet future change. With almost any current physical security solution, dedicated software and hardware combine to provide specific functionality. A change in functionality, therefore, requires both software and hardware development. Such systems don't allow for fast responses to changes affecting the industry. And they don't anticipate future needs. From a client's perspective, systems based on dedicated hardware and software require significant investment for changes to be made, making them inflexible and expansion unnecessarily expensive.

Adoption of open standards

In IT, the decoupling of hardware and software has been a proven principle for many years, and so has the use of open standards. The latter approach is now being adopted by the physical security industry. Almost all video management systems and cameras, for example, have adopted ONVIF standards. And, from an access control perspective, card technologies and readers are interoperable. Recently, a new standardisation protocol was introduced for integrating offline locks within access control systems (Standardised Offline Access Application – SOAA). The paradox is, the use of generic hardware will make it easier to implement these standards, as it only requires development of software not hardware.

The adoption of these standards offers many benefits to security system users, of which freedom of choice and dealing with legacy might be the most important. Introducing standards allows clients to mix and match not only the cameras they need or the card readers that best fit their budget, it also allows them to select the specific functionality that suits their security policy.

Transforming the industry

The adoption of both generic hardware and open standards will benefit clients significantly and, in fact, transform the industry. Uncoupling software from hardware allows manufacturers to respond faster to changes. Moreover, it will allow for innovation, as the time to get new products and features to market will decrease. This will allow the entire security industry to react to change quicker, and it will also encourage the industry to be proactive and innovative.

The adoption of open standards will, ultimately, result in a different type of competition. Openness will make products more transparent and create fair competition focused on added value, unique features, product usability, design and innovative ideas, instead of hardware prices.

Nedap Security Management

Daryn Flynn

Business Development Manager

