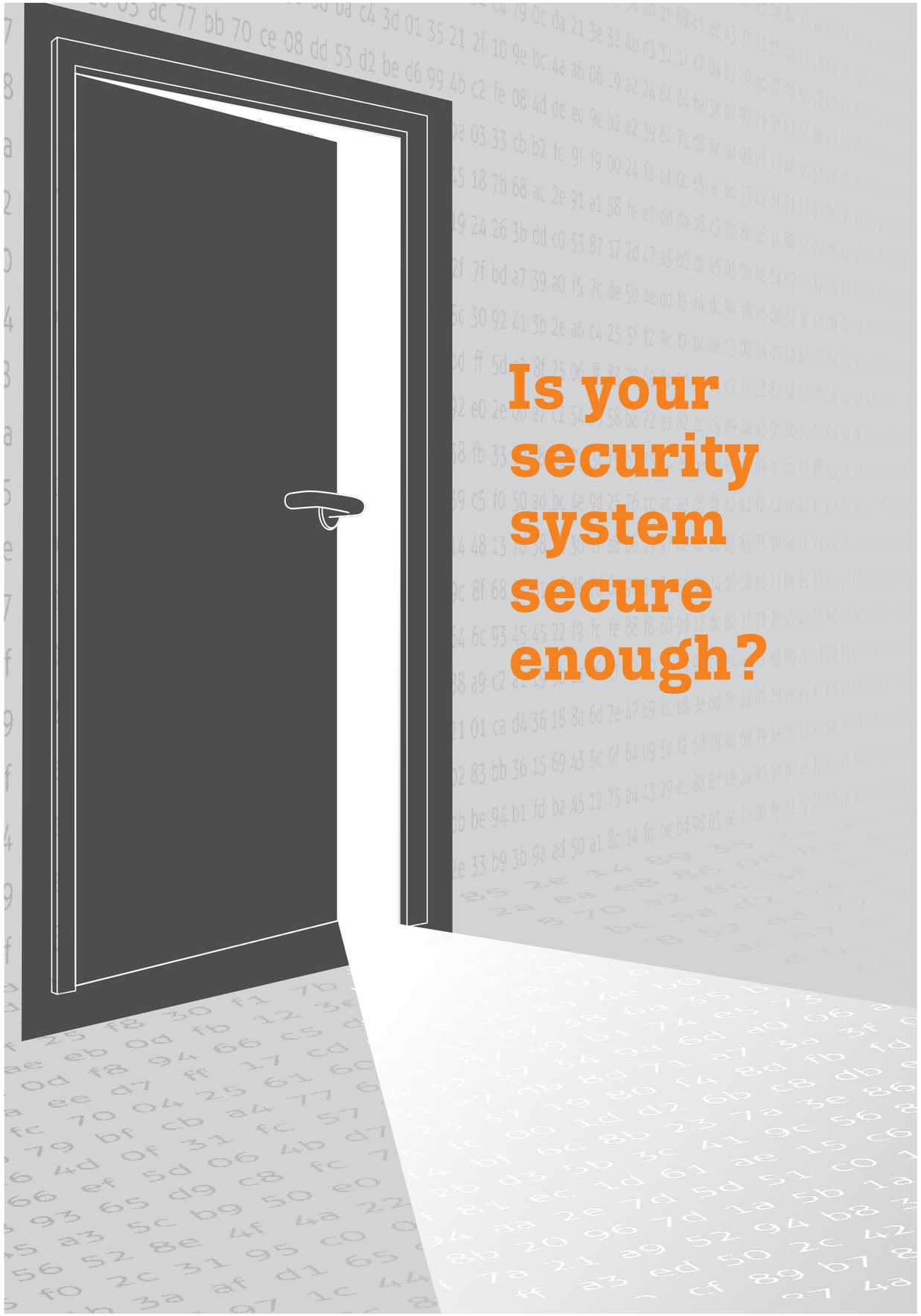
'Security is often seen as an asset that companies simply 'just need'. A cost rather than an investment, and for that matter, regularly undervalued and underestimated. Consequently, many companies start to consider the exact security measures that should be implemented within their company too late. The same applies to other facilities within organisations, such as IT. This is why in many fields, principles are developed to guide business decisions. Derived from best practices, principles offer guidelines for decision-makers and installers of a company's assets. These principles compel stakeholders to formulate objectives and define the project in an early stage. For that matter, principles serve as a foothold during the entire purchase process and implementation of acquirements.'

Nedap Security Management
Albert Dercksen, R&D Director

Security by design or designed for security?

With the worlds of IT and security merging and issues like globalisation , new ways of working and technological developments, the 'security' of security systems is getting more demanding. Consequently, security principles are getting more important. That's why proven security principles are derived from IT security.

Security principles can be defined as the collection of desirable system properties, behaviors, designs and implementation practices that attempt to reduce the likelihood of threat realization and impact should that threat be realized. Security principles help derive requirements, make architecture and implementation decisions and identify possible weaknesses in systems (OWASP, for example). They support security decision makers to contemplate on how to create a secure environment right from the moment a need for security is identified. They force procurers to be critical and constantly question the decisions made during the purchase and implementation of security measures .



Is your security system secure enough?

Proven IT security principles apt for physical security

The following principles from IT security may apply to the selection and implementation of physical security measures, depending on the type of security system under consideration:

Apply defense in depth

That is, multiple layered security measures are needed, no-one should rely on a single point of protection, public access to the system should be isolated from its mission-critical resources and physical and logical measures should be combined.

Use a positive security model

Instead of using a black list, a white list should be utilised to secure controlled access, in combination with fail-safe defaults and minimised attack surfaces, e.g. the use of pre-defined options rather than free fields to fill for data-entry. Ensure the implementation of a failsafe policy and all components run with least privilege.

A system's components shouldn't have more functionalities than needed to perform its tasks

For example, any component should be enabled to access tables in its databases needed to function and not all tables or databases in order to preclude unauthorised access.

Avoid security by obscurity

In a well-designed cryptosystem, only the key needs to be secret and the algorithms used must not contain any hidden secrets. For that matter, verifiable and economically healthy mechanisms should be used. And the efforts and investments should offset the obtained levels of security.

Detect intrusions

Make sure to log all relevant information to act upon events once they happen. Also, implement procedures for consequent monitoring and responses to events.

Don't trust infrastructure or services

Whereas any external asset or service needs to fit the organisation's policy it should be verified. Besides, all external systems should be treated with caution using similar standards.

Establish secure defaults

Security should never be compromised by usability. By default security measures should be as high as possible. The system should enforce this, whilst specific users are allowed to make exceptions when needed. This should be regulated by the system.

Keep it simple

Whilst security can never be compromised by usability, complexity will compromise security. Consequently, security and level of complexity should be in balance, that is, the user-friendliness as well as the system's architecture and possible integrations. Working with a complex system results in too many dependencies jeopardizing security.

The mission of the security system should survive an attack,

not its different components. That is, the system as a whole should be secure, not each individual component.

Applying security principles

In order to be useful to select and implement security solutions, security principles should be evaluated, interpreted and applied to address a specific problem. By evaluating and interpreting each principle, many of the threats to a security system are discovered and ultimately a set of protection requirements may be derived. The goal is to end up with a complete list of what is required to offer the service securely. It should be noted that this complete requirement list is specific to the problem which needs to be solved, also referred to as the 'security target'.

'From a manufacturer's perspective we found that the use of security principles shouldn't be confined to the product selection and implementation as they service during the entire product development lifecycle. It's our task to ensure our customers implement security measures that meet their wishes and requirements as well as local laws and budget constraints. From this perspective, we've adopted security principles to enable our customers to meet their ultimate objective: creating a secure environment and tracking and tracing all people that enter their company. '

Nedap Security Management
Matthijs Schippers, system specialist

Principles for development

The big challenge for the security management product vendors is that they should offer solutions to many- sometimes contradictory- requirements posed by their customers. The call for commercial off the shelf security management products forces the vendors to implement feature-rich, flexible, usable, and adaptable products which can help secure a wide range of security targets and must abide the security principles in the way the customer has evaluated, interpreted, and applied them. The only way to achieve this is to offer products which are highly configurable and adaptive. That's why manufacturers should inherently abide well defined security principles. Currently, they offer security by design whilst systems should be designed for security.

Want to read more about
how to secure your security system?
www.nedapsecurity.com