

## secure solutions

[commissum - that which is entrusted]

**optimum end-to-end security can only be achieved through security being a fundamental element of architectural design, incorporating a proper understanding of the interdependence of technology with the management aspects of security**

### issues

Security is not just about technology; technology is however an important element in most effective security architectures, appropriately integrated with policy, process and management. It is absolutely essential when selecting technology products, and designing technology based solutions, that the importance of this interdependence with the management aspects of security is properly understood.

Many organisations focus on technology when implementing their information infrastructure; frequently, it is often developed over time, with security added as an extra at a point in an organisation's growth where the risks start to be acknowledged. This is frequently achieved by adding discrete security elements such as firewalls, authentication, VPN, etc, in a piecemeal fashion.

This is far from ideal, and can lead to a security architecture that is both complex and by virtue of this complexity inherently insecure. Internal IT departments may not have the specialist knowledge and rarely have the spare capacity required to properly plan and implement an integrated, secure solution appropriate to their organisation, in a phased way, over a period of time.

### approach

Truly secure solutions require security to be a fundamental element of the overarching architectural design – derived from proper risk assessment, and linked to appropriate policies and management processes.

A **commissum** Security Architect will work with your design team to plan and achieve an optimum solution for end-to-end security. The approach will be pragmatic, acknowledging and embracing legacy systems, but essentially adopting a forward looking approach to designing a solution that can continue to grow securely as the business grows.

The approach has to be flexible to take into account varying business models, risks, etc, but typically would include:

- establish business requirements - identify key assets & analyse risk scenarios to focus security strategies
- analyse legacy systems with respect to fit with future strategy and potential technologies
- cost benefit analysis – various solutions & phasing
- security architecture design & technology selection
- plans for implementation
- periodic review, accommodating change - environment, business model and technologies

### customer benefits

A "designed-for-security" solution road map is produced that provides appropriate security levels, phased throughout an organisation's development.

Security is hence implemented as part of an integrated solution. When compared with traditional "bolted-on" solutions, the security architecture will be:

- inherently more reliable & secure
- cost effective
- planned with growth in mind
- more adaptable with respect to future technologies
- backed by the knowledge of experienced security professionals

**“Yes – a bulletproof vest.”**

James W. Rodgers (1911-1960)  
When brought before a firing squad and asked  
if he had any last request