

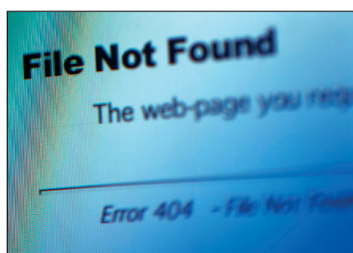


## • Security Infrastructure Design

- Internet Gateway Architecture
- Data Center Security Design
- In-situ Infrastructure Hardening
- Secure Deployment Process

### Introduction

Information Systems security like physical security, is most cost effective when designed-in from the outset. However not every company has the foresight to do this and many IT suppliers still do not have security as a primary concern when bringing their products to market. The networking boom of the late 90's resulted in the rapid deployment of thousands of servers, switches, and applications as companies connected to the Internet, automated supply chains and issued laptops to mobile workers. Little thought was given to the likely ongoing cost of managing security for this huge new infrastructure.



Today IT managers face increasing malicious activity, a stricter regulatory environment, and a new awareness of personal privacy issues by their customers. This is reflected in the explosion in reported

incidents to the Computer Emergency Response Team (CERT).

By re-visiting the design of your existing security and following best practices in new deployments you can gain maximum benefit while making ongoing management less draining. Having a clear architecture, and making the most appropriate use of products and services you can reduce your exposure to risk while being able to 'do more with less'.

Our consultants have been working in the field of security since 1995 and have architected Backbones, LANs, and Data Centers for the world's largest Internet service providers, protecting tens of thousands of customers worldwide.

### Approach

We understand that every business and industry is unique and that every project will require a tailored approach. Our success formula is based on listening to individual client needs, and from this, building an effective delivery framework from a vendor neutral position.



We believe success in business is built on relationships that are founded on trust, clear lines of communication and coordinated action, supported by technology. It is your business and we believe in providing the complementary skills, approach and tools to deliver against your objectives while ensuring you

retain control over what is happening. As a result, we enjoy repeat business from satisfied clients who endorse our reputation as world-class professionals by getting us to do what we do best, deliver.

Our goal is to increase security without damaging productivity.

Firstly, ascertain precisely what you expect from the engagement, and clarify these requirements in a scope document.

Gather information on the existing IT environment. This phase will be conducted with the minimum disturbance to systems and staff, via documents, interviews, and hands-on investigation.

The deliverable takes the form of a recommendations report and optional project plan. Depending on the client's requirements this phase may involve the hands-on project management and implementation of the recommendations on your live systems.

### People

Our consultants are experts, having worked previously in senior security roles for the worlds largest and most successful ISP. With an estimated 70% of the Internets traffic passing over their network, they deployed and managed thousands of systems securely for blue-chip Times Top 100 and Fortune 500 customers. We have advised a number of public bodies including the Financial Services Authority and the Criminal Intelligence Units of a major UK police force. Staff are highly referenceable via previous engagements with top 5 Investment Banks, Telcos, Security vendors and ISVs.

All our consultants have previously occupied positions of responsibility within organisations where the buck stopped with them for security management.

### Research & Technology

In order to keep abreast of the latest developments in attack and defence technology, we carefully monitor security newsgroups, mailing lists, web sites, and chat rooms. In addition to this, we operate a number of Internet connected systems in the UK and abroad, each of which records hacker scanning and infiltration attempts against OS and popular 3rd party applications. During the execution of our duties we routinely use a mixture of open source, commercial, and in-house developed tools.

### Industry Expertise

We have participated in a number of large industry-wide projects including the GPRS Roaming Exchange (GRX) the Automotive Network Exchange (ANX) and the European Automotive Network Exchange (ENX). All of these projects mandated complex security requirements for business critical infrastructure used by hundreds of commercial organisations 24 hours a day.

### Conclusion

Upon implementation of an improved design for security, you will be well positioned to cope with current business demands and unpredictable challenges of the future. A better design will reduce time spent fire-fighting allowing staff to be more pro-active. Sophisticated security systems should not need an army to run if implemented wisely.

#### **A better security design delivers measurable advantages;**

- Lower total cost of ownership for IT systems.
- More effective use of capital through efficient topology.
- Reduced frequency and impact of human errors or misconfiguration.
- Reduced impact of '0 day' vulnerabilities.
- Faster, safer new deployment of systems.