CST

An introduction into Information & System Security

Foundations & Essentials

Network Security

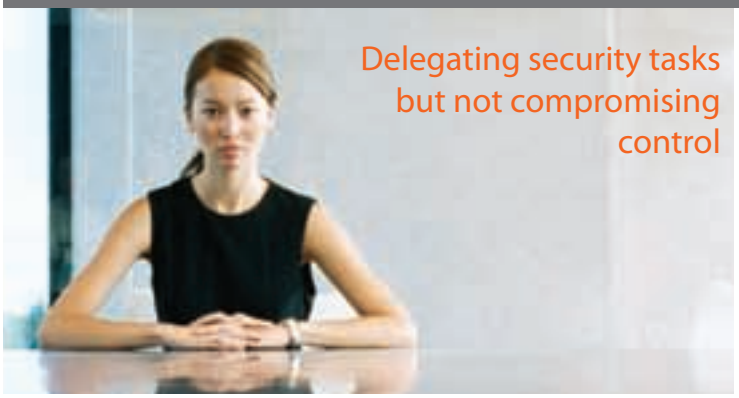
A productive IT network should control abuse from all its quarters

Network Security is more than just security solutions, pragmatic policies and processes are equally as important. This coupled with ever changing business needs and resource pressures compromise the risk values.

In our experience most organisation have a desire to have a strong security posture but lack the resources and expertise to have a dedicated IT security Dept. or function, it's CST that can fill such a breach.

Out Tasking Services

Managed Security



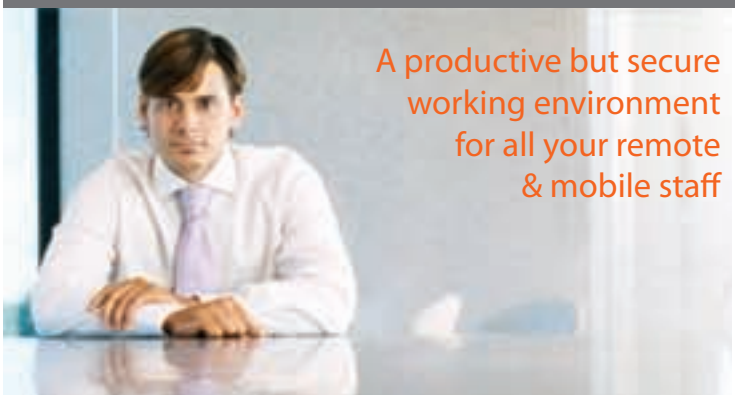
Delegating security tasks but not compromising control

In most instances security requires resource and expertise to obtain the maximum return from its investment. Ironically in most organisations, such resource and expertise can not be spared; the effect is a compromised investment.

The ability to subcontract or "Out Task" is one resolution to the problem.

Extending The Working Perimeters

Remote & Mobile



A productive but secure working environment for all your remote & mobile staff

Organisations needs to be more effective and productive and this lends itself to enabling staff to work from home, equipping staff with laptops so they can travel and using mobile devices like PDA's.

Securing remote and mobile working is essentially about allowing the productive access of network assets safely to external parties outside of the physical perimeter.

Core Practices & Technologies

Network Administration

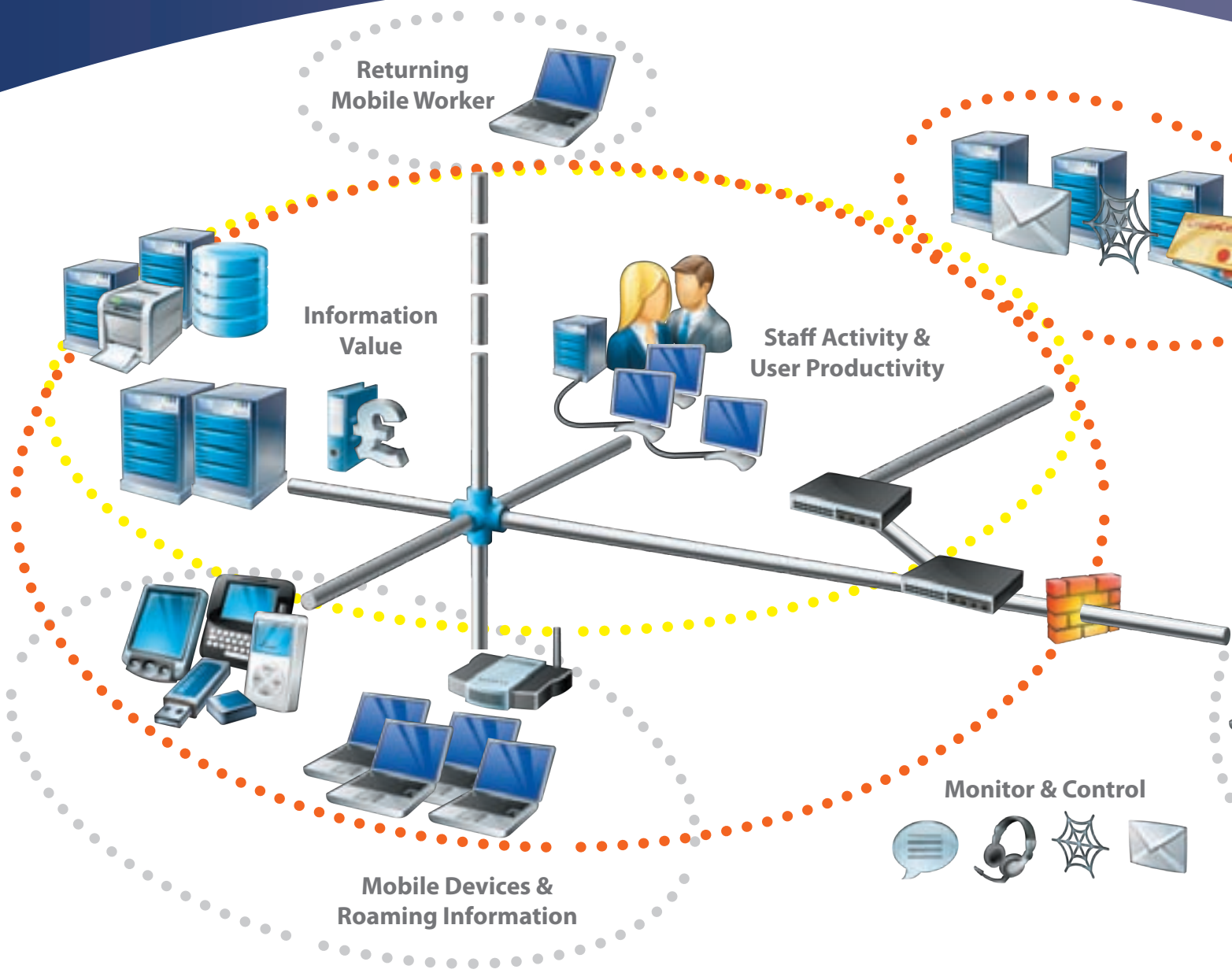
Good network house keeping creates a sound security posture

Network Administration may not obviously appear to a security discipline, but if you accept that:

" Good Network Housing Keeping
= A Sound Security Posture "

then it makes sense for CST to supply and support a set of key tools that provide just that. Administration embraces issues like: patching, recovery, backup, configuration control, password management and deployment.

Information & System Security



Physical Perimeter		Traditionally rested at the boundary confines of the office or building
Virtual Perimeter		Extended physical boundary to any network addressable host
Projected Perimeter		Maintaining security standards to all end points regardless of location

CIAC ***is an acronym to understand & define IT security***

Confidentiality
Protection of information from unauthorised disclosure or interception

Integrity
Safeguarding the accuracy, completeness and consistency of information

Availability
Ensuring users have access to systems and information when required

Compliance
Conforming to relevant customer, industry, and statutory regulations

Security Management & Posture

Recommendations are based on eleven years industry experience with the insight of international security standards like ISO 27000 and the demands of customers requiring a system to manage security rather than simply more burgeoning technology.

Key Organisational Framework

- Incident management
- Security review forum
- Explanation of responsibilities
- Risk assessment
- Impact evaluation
- Core operational controls: (Virus & malicious code, Perimeter access, server & work station configuration, User/management awareness and network access standards

Re-Active

- Perimeter access controls
- Malicious code defence
- Backup

- Network access controls
- Gateway content controls
- Penetration testing
- Business continuity plan

- Security policy
- Patching programme
- Network security
- Host security
- Data protection
- Exploit & vulnerability scanning

Pro Active

- Security system management
- User awareness/ education programme
- Security incident review
- Risk assessment
- Log analysis

Operational Risk

Risk

- Fraudulent material loss
- Loss of image
- Customer loyalty
- Shareholder confidence
- Operational ability
- Industry ranking
- Staff grievance
- Systems efficiency
- Statute & civil legal action

Countermeasures (C)

- Formal security policies
- Proactive exploit scanning
- Vulnerability intelligence
- Threat detection & prevention
- Staff knowledge & awareness
- Access control standard
- System organisation
- Information Security Management System (ISMS)

$$\text{Risk} = \frac{V \times T}{C} \int AV$$

Understanding the components that equate and comprise risk, is the first step to a risk management programme. An organisation can not eliminate all risk, but instead have to accept a level appropriate to their own particular operating needs.

Vulnerabilties (V)

- Exploitable conditions
- Remote & 3rd party access
- Gateway & system controls
- Staff knowledge
- System misconfiguration
- Distributed information
- Management policy
- Weak passwords

Threats (T)

- Opportunistic fraud
- Pre-meditated attacks
- E-commerce deception
- Disgruntled staff/customers
- Phishing attacks
- Staff ignorance
- Competitors
- Media & press

Asset Value (AV)

- Intrinsic value of data
- Loss of availability (email, website, finance, stock)
- Disclosure of information to public/customer
- Unproductive system use
- Cost of replacing assets
- Integrity of information

> No single vendor or product can secure your business.
>
> One independent specialist can.

Information & System Security

CST (Computer Security Technology) has over 11 years of dedicated IT security expertise - This makes CST one of longest established specialists in network and information security within the UK. We provide consultancy and managed services for IT departments who may lack the time, resources, or expertise themselves. CST is here to compliment your own resources and help fill any resourcing and skill gaps within your own security posture.

CST is keen to build and maintain robust relationships with customers; we feel it is important to have a good level of trust as we are working with sensitive customer information. CST's typical customer engagement commences with a project based security assignment, in time this leads to mutual trust and confidence which in turn results in CST typically becoming a trusted adviser for objective advice and pragmatic assistance, all of which is independent from any security vendor and delivered without the industry rhetoric.

To meet such diverse requirements CST has created distinct services that together form a security umbrella of expertise, this includes:

- **Security sector accredited staff**
- **Onsite security tool kit installation**
- **Associated configuration consultancy**
- **Security Manager out-tasking**
- **Emergency incident call-out and containment**
- **Policy review and security management guidance**
- **Risk Assessment embracing information asset quantification**
- **Managed Security Services (MSS)**

Tel 020 7621 9740 | **Fax** 020 7621 9730 | **eFax** 0207 099 6878 | **Email** info@cstl.com | **Web** www.cstl.com

Computer **S**ecurity **T**echnology Ltd. 1st Floor, Asia House, 31-33 Lime Street, London, EC3M 7HT