

Infrastructure Security: Network



**PROTECT
SERVICE**

Improve corporate risk reduction with strategic security and privacy services.

Is the Security Strategy and Management Service right for your company?

- Are your network decisions guided by a long-term IT and security strategy?
- Is your network “secure-by-design”, or are security features added on an *ad hoc* basis?
- Are your existing technology controls sufficient to secure your data?
- Are you presently upgrading your network, and planning to implement new security technologies?

Overview

Your organization’s network infrastructure provides the functional support for secure business operations – how can you effectively use it to create a competitive advantage?

Digital Defence will assess your network infrastructure, or specific components, using a methodology based on the international standard ISO 27001:2005, or the [Sherwood Applied Business Security Architecture, SABSA](#). The primary characteristic of the SABSA model is that it is risk-driven, and all aspects of the analysis are directly derived from an assessment of business requirements.

We provide an objective assessment of the effectiveness of your network ‘s technology, people and processes, and how they impact your organization’s data security. Our goal is to ensure that the most appropriate controls are implemented— your business strategy is fully supported, security and manageability are enhanced, and complexity and cost are reduced.

Benefits of a Secure Network Infrastructure

- Develop the ability to prevent, detect, and respond to network attacks; reduce or eliminate financial and reputational costs of a security breach
- Optimize security and management costs; as much as 50% in annual savings
- Ability to effectively plan near-term and future security investments in network architecture
- Access to Digital Defence’s Trial and Evaluation lab to validate the effectiveness of your network components and architecture prior to implementation; ensures most cost effective solution and rapid deployment
- Comply with Federal and industry regulations; meet audit requirements

Technologies Secured

- Wired networks (WAN, LAN)
- Wireless networks (WAN, LAN, Bluetooth)
- Virtualized environments, including “cloud computing” platforms
- Remote access technologies (IPSec, VPN, application-based)
- Network and security devices, including firewalls, VPNs, IPS/IDS, network access controls (802x/NAC)
- Mainframes, servers, workstations, and mobile devices
- Storage area networks
- Encryption systems; hardware and software
- Voice over IP (VoIP) networks, PBX, and related telecommunications
- Industrial systems (SCADA)

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or “ethical hacking”. And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

A secure-by-design network architecture will minimize security risks and improve resilience and manageability; cost savings can exceed 50% annually!

Service Description

During the infrastructure security assessment, DigitalDefence will:

- Assess strategic, security and network documentation
- Review the existing network architecture
- Conduct a data flow analysis to identify where data enters and leaves the controlled network, including third party connectivity, backups, DRP/BCP sites; review separation of production and test data
- Conduct a network technology review, including the existing network topology, access controls, authentication mechanisms, and network administration and maintenance; this review will include relevant people and processes
- Review physical and logical security controls for servers, workstations, and mobile devices
- Assess security log and event management systems; ensure auditability
- Assess resilience and survivability of the network

DigitalDefence can provide additional services to improve the security of your technical infrastructure, including:

- Assistance in product testing and selection
- Installation and configuration services, including pre-staging
- Hardening of network equipment, servers, and workstations, including creation of a Common Operation Environment to facilitate rapid roll-out of secure network configurations, system “builds”
- Centrally managed and auditable vulnerability and patch management
- Vendor-specific training

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.