Chapter 17

SHIELDING YOUR ASSETS

INTRODUCTION

Many enterprises, especially small and midsize enterprises, can afford neither the security products nor the requisite expertise to derive full benefits from them. What they need is an effective perimeter solution that does not require hardware, software or installation [1].

THE BUSINESS ISSUES

Internet-perimeter security is a high-wire act in which enterprise owners and executives must balance the price of security versus the risks and costs of failure. The price of security can run into tens of thousands of dollars for capital expenditures (CAPEX) and ongoing investments in:

- Security hardware such as firewalls, intrusion detection/prevention devices and sensors that must be installed, monitored and maintained
- Security software that must be installed, configured, and managed for updates and patches
- Full-time employees to install, monitor and manage the equipment and software around the clock
- Consultants using specialized security expertise to adapt these security solutions to the needs of the business [1]

The costs of failure are even more painful and include:

- Damage to the enterprise and its networked systems from threats such as worms, viruses, Distributed Denial of Service (DDoS), identity theft, phishing, directed and undirected attacks and unforeseen zero day threats
- Network downtime resulting in lower operations productivity and reduced employee efficiencies
- Lost revenue and lost customers from the interruption in enterprise continuity

- Damage to enterprise brand image and reputation that could lead to loss of credibility among stakeholders both inside (board of directors, employees) and outside (customers, partners, regulators, media) of the enterprise
- Legal consequences (stiff fines and jail time) stemming from non-compliance with government regulations that require enterprises (regardless of size) to protect the privacy and integrity of customer and employee data and other digital assets [1]

To attain and sustain Internet-perimeter security is especially challenging for small and midsize businesses (SMBs). For these enterprises, achieving levels of security that are comparable to that of a Fortune 500 enterprise may seem unrealistic. The costs of failure, however, are unacceptable (with less margin for error than many larger enterprises have) and include everything from the consequences outlined in the preceding to the potential demise of the enterprise. Today, SMBs must work hard to find the right balance of security investment and cyber-risk for their enterprises [1].

What is the typical security profile of an SMB? It depends. SMB security solutions are as varied as the businesses themselves. The SMB market covers a broad spectrum and means different things to different people: SMBs generally are considered to have from 100 to 5,000 employees. Their security setup may be as simple as having a firewall and a network administrator to having an array of equipment and a Network Operations Center (NOC) supporting multiple networks across geographically dispersed locations [1].

Even with this broad range of SMB security environments, there is still common ground in the security issues with which these enterprises must deal. SMBs all have needs, issues and challenges, pertaining to computer security that include:

- Security policy set-up, management, and governance
- Vulnerability shielding of assets and patch management
- Security resources, including in-house security expertise (or lack of same)
- The challenge of keeping up to date with infrastructure updates
- The difficulty of staying current on the dynamically changing threat environment
- Validation and remediation of security events
- Regulatory compliance (the need to satisfy the requirements of governmental regulations such as Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Statement on Auditing Standards (SAS-70), California Senate Bill 1386 (SB1386), ISO 7009 and Canada's Personal Health Information Privacy Act (PHIPA))
- Pressure from various entities, including the enterprise's board, auditors, competitors, media and regulators [1]

CONVENTIONAL SECURITY SOLUTIONS

What choices do SMBs have when it comes to protecting their networked systems from Internet-based threats such as worms and viruses? Historically, small and midsize enterprises