Perhaps the greatest threat to any organization in this internet, digital, and electronic age is a breach of the network and the subsequent negative consequences. A breach of your network presents costs which may include: legal liability, negative publicity, and down time.

As profit margins shrink and the cost of securing networks rises, many CFOs are waiting and analyzing why they should or should not implement network security.

Network security is no longer a tough sell, and CFOs might well regard the enormous and growing importance of having a more secure network. Data protection is necessary, and to cope with this likely scenario, you will need to understand real security threats. Studies have found that 72% of breaches occurred because of a lack of protection, with 14% occurring because of malicious or insider threats.

To meet best security practices for your network, it is now necessary for CFOs to:

1. Have reasonable and workable security policies and procedures
2. Know your technical (IT) team and their skill sets
3. Assess your company security before attackers do
4. Have detection and monitoring systems to identify activity in your network traffic. Also have detection and monitoring systems on electronic devices and hosts within your network
5. Incorporate the following essentials when budgeting and designing your network:
   a. Security
   b. Growth
   c. Interoperability
   d. Ease of use
   e. Low maintenance

Dynamic business models require dynamic enterprises. The e-business world is changing, and companies can no longer rely on traditional methods to protect their e-business and their network. Firewall and virus protection are not the “Holy Grail” of network security any longer.

The more innovative CFO will rely on new techniques - perhaps even using ones derived from gaming - as a means to move forward with the management of data confidentiality, integrity and availability.