Reducing the Cost of Compliance

The American Heritage dictionary defines compliance as "*The act of complying with a wish, request, or demand; acquiescence*". When you think of complying with something, do you normally consider it a wish? So, would paying my taxes indicate I'm complying with the Federal government's *wish* that I pay my taxes, or is it a *demand*?

Before we talk about the specifics of how to manage and control the costs of compliance, let us review some of the major compliance legislation faced by organizations today:

- Gramm-Leach-Bliley Act (GLBA) – 1999
  - Financial Institutions.
- Health Insurance Portability and Accountability Act (HIPAA) – 1996
  - Health Care Industry.
- Sarbanes-Oxley Act of 2002 (SOX) – 2002
  - Publicly traded companies.
- Payment Card Industry (PCI) Data Security Standards (DSS)
  - Credit Card processors.

As you might imagine, the verbiage of some of these Acts is sometimes vague and often leaves the reader without a clear idea of what the original idea was supposed to be. When you read these documents often times a particular recommendation is listed as "should have" or "might have". What does that mean? Given a choice, the average business owner doesn't **choose** to spend money freely. So how do we save money and still be compliant?

How about starting with common sense? The real goal of this legislation is to protect the users from the system. Whether those users are patients in a hospital or investors buying stock from publicly traded companies, the goal is to protect the confidentiality, integrity and availability of the corporate resources. When you talk about compliance, the real litmus test is "due diligence". If you have a problem, did you at least try and implement the internal controls specified by the legislation? If not, you're probably in a lot of trouble.

Technology certainly has a place to play in the compliance equation, since a large part of the problem is protecting data in motion and at rest. If you are one of the unlucky ones to have to deal with multiple compliance issues, your best bet is to look for underlying similarities in the documents. A tightly controlled firewall and IDS technology from your favorite vendor will probably help you check off a box in each of the above mentioned compliance documents. Effective network management, well-written policies and procedures and a comprehensive security management plan will show due diligence no matter what regulations your organization may find itself under.

The bottom line is no matter where you fit into the compliance hierarchy; don't wait until you have a problem to start the process. Carefully read the specifications and determine what has to be done, what should be done and what might be done if you really have a lot of money. Remember the due diligence test and always look for ways to consolidate requirements when spending money for new technology. Wherever possible, look for non-technical ways to satisfy requirements.