



**Providing Regulatory-Compliant Telecom Solutions**

By Dan Blacharski

Corporate scandals, fiscal mismanagement, and insider trading make great headlines, and the attention these misdeeds received has resulted in a raft of new regulations, designed to prevent those at the top from making similar grievous errors in judgment. Laws such as Sarbanes-Oxley and others are strategic moves to prevent a major disaster, the likes of which we have not seen since the Crash of '29.

Many regulations are specific to a certain group of businesses. Sarbanes-Oxley presents mandates to publicly-held corporations requiring them to ensure the accuracy of financial statements. But the effects go much further. In most cases, companies must not only ensure that they themselves are compliant, but also ensure that their partners and suppliers, including those that supply telecom solutions and infrastructure, are compliant. As conduits of the information being governed, telecom providers are perhaps the ones who are most affected by these new laws.

"The pressures of compliance are definitely affecting US enterprises and their demand for specific telecom and networking services from providers," notes Chris Neal, Research Director at Sage Research. Beyond establishing compliance internally with their own systems, these regulations impact telecom service providers in "...any outsourced solution that involves the transfer or processing of relevant data and information for enterprise customers."

**Why Telecoms Must Adhere**

Regardless of whether they are directly mandated by specific legislation, telecoms above all other types of providers must provide compliant solutions to their customers that are under mandate. With the internal controls mandated in Sarbanes-Oxley's Section 404, it's about protecting the integrity of financial data and ensuring that it is not compromised. It becomes necessary for telecoms to offer those who must face these new mandates, solutions that help them to comply.

While some telecoms are making strategic partnerships with security companies to resell security services, others are buying them outright. MCI, for example, recently acquired managed security services provider NetSec. Forrester Research notes that "NetSec's Finium SEM platform lets MCI gather and aggregate data from sources like its IP backbone and its managed private networks. Thus, MCI will be able to offer its customers improved security intelligence on par with other IP backbone providers like Sprint and AT&T."

**FCC Regulations Aimed at Competition**

In addition to dealing with these regulations, telecoms and cable companies must also face FCC regulations aimed at creating competition, by requiring larger, traditional

## **Providing Regulatory-Compliant Telecom Solutions**

providers to allow smaller competitors, ISPs and VoIP providers to lease their networks for a fee.

Arguments currently being heard in the Supreme Court may call for cable providers to be required to lease their lines to rival ISPs as well. The cable industry is arguing that such regulation would be a disincentive to rolling out additional broadband services; most cable companies currently only offer customers their in-house ISP. Competing ISPs claim the regulation would provide consumers with more choices, as has been the case with telcos. The way companies compensate each other to use an ILEC phone network has always been a subject of heated debate, and the increasing acceptance of Internet telephony has brought this debate to the forefront.

Newer services such as VoIP may have enjoyed a brief period of unregulated activity, but it didn't take long for VoIP to pulse onto the competitors' and regulator's radar screen. VoIP provider Level 3 Communications is an example of increased dealings with regulators. Most Internet phone calls either originate or terminate on a traditional phone line, and providers like Level 3 must compensate the phone company accordingly. The amount Level 3 and other VoIP providers must pay the local telcos however, is subject to regulation. Recently, the company withdrew its petition to the FCC, which asked that it be exempt from paying the higher access fees that conventional long-distance companies pay local telcos--not due to any change of heart on the part of Level 3, who naturally wants to have lower fees, but because of the change of leadership that just occurred at the FCC. Ultimately, the rates VoIP providers pay local telcos--and indirectly, the price of VoIP service itself--will be determined by the regulator.

### **Impacts on OSS**

A telecom's OSS keeps an infrastructure running smoothly, controlling accounting functions and configuration and interacting with the network infrastructure. Because this carries with it the need to transmit sensitive personal and financial data electronically, billing applications, in particular, are sensitive areas in terms of the information they contain.

As such, identity management and access control to the OSS becomes a vital part of the infrastructure; within this realm the functions include identity management and user provisioning. Resources within the OSS must be provisioned, such that a policy of "least access" is enforced, granting each employee access to only what they require to do their jobs.

In larger organizations, this is best done through a role-based model, rather than provisioning each employee individually. "In situations where compliance calls for strong authentication, token-based systems afford the greatest measure of protection, but also the greatest mobility and flexibility for users," notes Paul Ardoin, Product Marketing Manager at Secure Computing Corporation. "In some circumstances, an official memorized password policy may be adequate. However, in the case of a telco requiring a secure system for governing access to the OSS, there will be sensitive personal and

## **Providing Regulatory-Compliant Telecom Solutions**

financial information that will likely fall under the purview of one or more regulations, either directly or indirectly....”

### **Interoperability and Security**

Telecom companies and other service providers must be able to share critical information, such as customer data, for this interoperability to take place. Local Number Portability (LNP) is an excellent example of data sharing between telcos. When a customer wants to change providers and keep their same phone number, several changes in routing and OSS are required, and this requires cooperation between carriers during the transmission of personal and billing information, and must be protected internally by the telcos.

A new level of cooperation between telcos also points to the need for greater security and a greater need to check systems for compliance. Packaged service offerings that include interdependent services from multiple providers require an element of trust to be present, not only between customer and service packager, but between the service packager and each provider. To facilitate this trust, requirements that include confidentiality, privacy, and security are paramount. All telecom companies will be required to deliver on these areas as a core attribute of their service offerings.

The regulatory environment has had a great impact on business in general, and on telcos in particular. Going forward, corporations will be looking to their telecom providers, more than any other partner, for assurances when it comes time to certify their compliance with these regulations.