"The Information Security Threat from Within"

Topic: The greatest impact on network security in the next 5 to 10 years will come from the social norms and habits of computer end users. Distributed and mobile computing environments are highly susceptible to dynamic and sometimes destructive user habits that emerge with changing social norms.

Abstract: Human nature is the reason the enterprise should monitor its employee network and Internet use. Individual computing has moved from client server to desktop, then to laptop and now to mobile devices. While some networks may not be fully distributed, most end users operate that way. Today's end users are touching the Internet and touching your private network in a myriad of ways. Socially, workers feel that they are working longer hours and therefore have the right to manage their own time. As such, employees may feel that where they go on the Internet and what they do when they get there is only their concern. However, the truth is what they did there and what they brought back to your network is your concern.

What mobile employees do when they are away not only introduces leaks in your security fabric, it exposes your enterprise to liability and risk. While you cannot change Human Nature, you can take it into account when you allow these mobile workers intersection with the Internet. Enterprises need to apply consistent, scalable and fair rules of conduct to the actions of all employees. Those rules need to apply across the entire network, especially extending out to the remote user of network assets.

Presenter: Joe Field, Chief Technology Officer of Pearl Software, Inc.

Joe Field helped found the internet monitoring sector back in 1996 when he and his team developed one of the first applications to help parents monitor the Internet activity of children on their home PC. In 1998 that technology received the Editor's Choice Award in PC Magazine. Joe's work has evolved into a scalable, enterprise class technology that is today being used by Law Enforcement to monitor the real-time activity of cyber-criminals and sex-offenders.

As CTO, Joe participated with Intel and Microsoft in developing WINSOCK II and the Service Layer Provider architecture. This development in 1998 was the foundation of the technology at the heart of Pearl Software's **Echo•Suite™ 7,** and the **IM•Echo™** and **Website•Echo™** modules. The Echo solutions are used by school, hospital, government and private sector customers to protect their networks from the results of unwise Internet use by employees.

Joe received his undergraduate and MSEE degree from the University of Delaware. He has conducted Doctoral research centered on the ARPANET and has been called upon to testify before Congress as an expert on Internet Monitoring. Joe holds several patents including technologies used to monitor PC communications and create safer Internet chat environments.