

## *Managing Risk and Security Efficiently and Affordably*

The security threats to banks extend from the lone high-school hacker to sophisticated, international crime rings and everything in-between. The challenges of protecting their Internet banking system are particularly intense for banks. All banks need a top-of-the-line service to compete in the marketplace, but many lack the personnel, expertise and capital to manage this vital, yet high-maintenance solution. The Application Service Provider (ASP) model is an ideal way for them to overcome these challenges and ensure that their online banking platform is secure.

As the threats become greater, so does the cost of security. Today, the entry fee for a truly vigilant security and infrastructure system averages \$700,000, with that number expected to increase tenfold in the next five years. Although that type of investment far exceeds the security budgets of most banks on their own, an ASP model scales this investment among multiple banks. Instead of a capital outlay, each pays a minimal monthly fee for world-class security expertly monitored around-the-clock.

A solid ASP Internet banking solution applies a full range of security technologies. The best way to illustrate the critical need for sophisticated protection is to explore some of the various types of security and the threats that can be prevented. The goal of Distributed Denial of Service attacks is to shut down Internet banking to its intended users by flooding the system with an unmanageable number of bogus requests. In this type of attack, criminals access millions of PCs around the world operated by organized crime rings. These computers are then directed to connect to the targeted Internet banking site at the same time. When these requests hit simultaneously, the system simply becomes paralyzed. No one, not even legitimate bank customers, can get through.

An ASP Internet banking provider will have a data center with multiple telecommunication lines with Distributed Denial of Service protection. It is nearly impossible to bring down a hosted Internet Banking solution because of its massive bandwidth and the fact that the circuits are load-balanced among multiple carriers.

In another kind of attack, criminals will employ micro-transactions to validate stolen credentials before attempting to move large amounts of money from account to account. A hosted Internet banking solution provider is constantly monitoring for these types of transactions, learns from other bank experiences, as well as other variances in expected and "usual" customer behavior and contacts the bank - who can contact the customer - when fraud is suspected. Finally, in an outsourced ASP environment, pre-established Service Level Agreements (SLAs) that guarantee performance should be insisted upon.

When it comes to protecting your customers' and your bank's assets from the multitude of threats constantly being conjured up by criminal minds with nearly unlimited resources, ASP offers peace-of-mind and unparalleled security. Harland Financial Solutions recommends an ASP model, such as that offered via its Cavion® Internet Banking solution, as the safest and most cost-effective means of deploying Internet banking to your customers.



**Jeff Marshall**  
Vice President

**Jeff Marshall** is Vice President of Strategic Technologies for Harland Financial Solutions. Mr. Marshall is a 1990 graduate of Colorado State University and is widely recognized in the software industry for his accomplishments, knowledge and vision. Harland Financial Solutions supplies software and services to thousands of financial institutions of all sizes, offering its solutions in both an in-house and service bureau environment. The company is a leader in core systems, item processing, enterprise content management, branch automation, CRM, BI, origination and document solutions, risk management, compliance training, financial accounting, open documents, mortgage solutions, card programs, EFT, fraud prevention, self service solutions and performance advisory services.

