

## *Finding a Balance between Security and Convenience*

Banks, large and small, are under daily attacks. Cyber-criminals and phishers are moving down the chain and targeting smaller banks because they are perceived as easier targets. They are also attacking consumers directly so there now needs to be a concerted effort across the board to protect customers' identities and accounts. Unfortunately, it is not a question of "if" but "when" your bank will be assaulted.

Everyone knows that security must be layered to thwart these evolving attacks, but it has traditionally been very expensive and difficult for bank IT staffers to implement and maintain numerous layers of defense. However, with the advent of Unified Threat Management appliances, banks can now deploy UTM devices that combine firewall, gateway anti virus, SPAM filtering, web content filtering, VPN and intrusion detection and prevention capabilities into a single platform. UTM is designed to protect users from blended threats while reducing complexity.

Even with UTM appliances in place, it is virtually impossible for banks to handle their security around clock with just internal resources. That is why so many hundreds of banks have turned to Perimeter Internetworking to handle their security infrastructure. We are far and away the industry leader in the number of security products and services – over 50 – that we offer. Plus because of our relationship with CUNA, all of our bank clients enjoy a discount off of our already affordable monthly rates. Whether they choose our Network (in-the-cloud) or customer-based services, banks are assured that our service will be continuously expanded, enhanced and upgraded for current and future regulatory compliance – 100% guaranteed.

Because today's threats are so dynamic and volatile, we developed a powerful tool to help banks understand their risks and prioritize their responses. Our Risk Profile system is built atop industry best practices gleaned from Perimeter's own decade of experience providing eSecurity to over 1,600 financial institutions. This program ranks a bank's business processes according to their importance to the organization and its vulnerability to financial, regulatory, and reputational impact. At the conclusion of the twenty minute questionnaire, banks receive prioritized recommendations on where best to mitigate risk, and where specific procedural changes will increase their security posture.

Just about every bank employee wears multiple hats during their day to day jobs, but security demands a full time effort and focus. That is why our managed security approach is growing in popularity so rapidly. As a single source provider, our bank clients benefit from a solution that offers a wide array of security services through one pre-integrated platform and web portal. The reporting capabilities are especially convenient for IT Departments when it comes to time to work with the auditors. It is just one more example of how we make security easily available and affordable for any bank that wants world class protection.



**Kevin Prince**  
Chief Security Officer

**Kevin Prince** is the Chief Security Officer (CSO) at Perimeter Internetworking™. In this role, Kevin assists with the company's strategic plan and is responsible for many of its strategic relationships. A well known expert in the security industry, Kevin regularly trains Federal Examiners at the Federal Financial Institutions Examination Council (FFIEC) on topics such as firewall security, remote access, virtual private networks, intrusion detection and prevention systems, and on what the examiners should look for when they examine a financial institution. Perimeter Internetworking™ is the leading provider of multi-threat, managed "Security in the Cloud" services to financial institutions and other firms with high data security and regulatory requirements.