

## Protecting Customer Data at Rest and in Motion

Given the difficult economic situation that we are currently experiencing, it is becoming even more challenging to protect customer data. Malicious acts by insiders always increase during recessions as people become more desperate and are tempted to take actions that they normally wouldn't consider. Unfortunately, there can also be an increase in inadvertent staff errors because oftentimes training budgets are reduced as a cost saving move.

A bad economy also affects vendors which is why examiners are significantly increasing their scrutiny of the way that banks conduct their third party relationships. Many vendors may reduce their personnel, scale back on their infrastructure, or even go bankrupt - all of which can adversely affect the bank. At Perimeter eSecurity, we have seven geographically distributed technical operations centers and three redundant datacenters which are validated by TruSecure, so our hundreds of bank clients never have to worry about our support levels or compliance certifications.

One of the most dangerous developments facing any bank today is malware implanted on web sites. There has been tremendous growth in this area because it is much easier than trying to break through a hardened perimeter that is protected by firewalls, IPS, etc. These powerful programs can wreak all manner of havoc once installed on a machine inside the bank, e.g., load keystroke recorders, launch other attacks, send unsolicited emails, and even provide full remote control to the attacker. In many ways, the users are compromising themselves, so it is incumbent upon the IT Department to protect their users as best they can. We offer a powerful Web Content Filtering Service that can block objectionable content while preserving access to valuable Internet resources. When used in conjunction with our centralized management of desktop and server virus protection, banks can leave individual employees out of the equation and remain secure.

Security Awareness Training is one area that banks should always view as a wise investment because it is one of the most affordable ways to reduce risk. We offer twelve courses that permit employees to learn on an as-needed basis at any time that is convenient for them. Vulnerability assessments are another ongoing requirement for banks, and our view of them is that they simply can't be a one-time event. Perimeter's Vulnerability Monitoring Service covers both external and internal monitoring and is effectively an audit of the bank's security installations 365 days a year.

Banks must remain vigilant regardless of the economy. That is why we make more than 50 different technologies available to them on a subscription basis. Perimeter's On Demand services, which are offered both on a network (in-the-cloud) and customer premise basis, are designed to be quickly and easily configured and affordable. More and more banks are choosing to work with us because they realize the benefits of partnering with a single-source provider that offers all services through one pre-integrated platform and web portal.



**Kevin Prince**  
Chief Security Officer

**Kevin Prince** is the Chief Security Officer (CSO) at Perimeter eSecurity™. 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 has been asked to train national and federal organization employees on relevant security issues over the years. Topics that Kevin has spoken on include firewall security, remote access, virtual private networks, intrusion detection and prevention systems. Perimeter eSecurity™ 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.