

## *Managing Risk and Security Efficiently and Affordably*

Banks should look to continually invest in security awareness and training of their employees because this is one of the most effective and low cost ways to minimize risk. Staff customers need to learn the 'what' and they 'why' of security issues so that they fully understand the liability, exposure and risks that the bank faces. Well trained front line employees are also able to help customers if they have questions about security and fraud related issues. Additionally, security awareness can be passed on to customers with brochures, website and email messages, etc that demonstrate that the bank is actively looking after the customers' best interests.

While phishing is still rampant, we are seeing an explosion of malware-infected websites. Compromising legitimate websites is truly a very effective technique, as is redirecting people to legitimate looking websites that are capable of infecting users' machines. Over the past year or so, we have seen major websites that receive millions of hits become infected with malware that can cause a great deal of damage simply by clicking on a link.

With the recession lingering, both fraudsters and employees can become more desperate. Outside attacks are on the increase, as is insider fraud. Many banks are cutting IT and security budgets at time when they can ill afford to do so. The bad actors continue to ramp up their activities, while overworked bank IT Departments struggle to find the time and expertise to protect their valuable assets. That is why we developed the Risk Scorecard that utilizes a Web-based tool to step banks through a process that helps them determine the best use of their budget. It recommends the next best security investment that will help mitigate the most risk based on their current situation.

Another extremely useful and cost effective service that we offer is our Quarterly Security Review. With this service, our security experts analyze virtually everything about a bank's security posture and come back with customized recommendations. This is one of our clients' favorite services because it saves them so much time, money and effort. Plus it delivers well written and thorough reports that the bank's IT Department can deliver to both their internal auditors and FDIC examiners.

Auditors are also currently very concerned about vendor due diligence, and this is one area where Perimeter E-Security really shines. Because we service over 2,000 financial institutions, we are under FFIEC oversight and work closely with them. This provides a great deal of peace of mind to our bank customers, along with the fact that we are financially stable. Even private industry has recognized our leadership position in the managed security services sector: We garnered a Five Star review from SC Magazine for our Firewall and Intrusion Prevention Service. With over 50 on demand security technologies that are straightforward and affordable to deploy, it is easy to see why we are the leader in managed security services for banks across the United States.



**Kevin Prince**  
Chief Technology Officer

**Kevin Prince** is the Chief Technology Officer (CTO) at Perimeter E-Security and spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise. With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk.

