

## *Managing Risk and Security Efficiently and Affordably*

The financial sector is the most exposed to targeted attacks - close to 40% of the financial industry suffers from Trojan attacks. Banks must continually focus on securing their customer data while complying with myriad regulations. There can be no letdown in the vigilant protection against unauthorized access to financial, customer, or transactional information -- whether it is mandated by Gramm Leach Bliley Act or a state data privacy and notification law, such as CA-1386 or to preserve customer trust and the bank's valued brand and reputation.

When it comes to minimizing risk, banks must pay particular attention to Phishing attacks because they have become some of the most common and most effective online scams for criminals. The schemes are varied, typically involving some combination of spoofed junk (spam) email, malicious software (malware), and fake Web pages to harvest personal information from unwitting consumers. Customers of well known and lesser-known banks have fallen victim to this pervasive form of online fraud. In fact, over the past 5 years, Cyveillance has detected phishing attacks against hundreds of banks across the country.

For banks, the total cost of a phishing attack is driven by the lifespan of the attack. Every hour that a phishing attack is live costs banks and their customers significant amounts of money. This theory has been proven with the simple fact that, in detecting and responding to phishing attacks, speed is the single most important factor in minimizing the cost of each Phishing attack. There is good news: many technologies, services and best practices implemented today can substantially minimize the impact of phishing attacks by limiting the time a phishing attack is live and reducing the amount of customers who unknowingly fall for these scams.

Cyveillance Anti-Phishing™ is a comprehensive, turnkey solution that enables banks to prevent, detect, respond to and recover from phishing and fraud-related malware attacks. Using our proprietary Internet monitoring technology, proven processes and procedures, and industry-leading security operations team, Cyveillance identifies targeted fraudulent activity such as suspicious domain registrations, phishing lures, spoof sites, malware distribution points and exchange of compromised credentials. Cyveillance Anti-Phishing is uniquely capable of detecting, processing and shutting down technologically advanced phishing attacks in virtually any language. Our anti-phishing services are backed by the industry's most aggressive Service Level Agreements (SLAs).

Based on 3rd party comparative studies and customer testimonials at multiple financial organizations, Cyveillance consistently outperforms every other solution on the market for both speed of detection and speed of response and shutdown, often shortening this lifespan by hours or days compared to other solutions. This reduction in the lifespan of phishing attacks will directly result in substantial cost reductions for banks which one of the many reasons why so many banks across America have chosen to partner with us.



**James Brooks**  
Director of Product Management

**James Brooks** is Director of Product Management for Cyveillance, Inc., where he is responsible for the strategic direction of the company's products and services. James has over 14 years experience in the security products and services industry. He has served in a wide range of functions and possesses a thorough understanding of the most current security technologies, network and Internet environments, and cyber intelligence strategies. James has been a noted expert on emerging online threats and has been quoted in several publications including Business Week and eWEEK as well as a featured speaker at recent CERT, SANS, ACFS and MRC industry conferences.

