

## *Securing the Bank from the Inside to the Outside*

Certainly the place to start with any community bank security strategy is the perimeter. Everyone connected to the Internet is a target, and we all face a nearly constant barrage of automated and often sophisticated attacks. But the focus on the perimeter has resulted in what is known as "candy bar security"... crunchy on the outside and all soft and chewy on the inside.

Meanwhile, the insider threat accounts for anywhere from sixty to eighty percent of all network breaches and simply can't be ignored. Attackers know that your workstations are the most vulnerable part of the network so they target your employees with a variety of enticements designed specifically to fool them into visiting compromised websites or installing malware that provides the attacker with a base of operations inside your network.

Additionally, insider abuse is also a very real threat. The knowledgeable insider knows your systems, and precisely where to find the data that's most valuable or potentially most disruptive.

There is an old truism that states that "you can't protect what you can't see," so visibility is the key. How do you know if the security devices and applications you have deployed are effective? How do you know if the policies you have created are being enforced? How do you know if there's something suspicious or malicious happening on your network?

All of the network and security products that community banks have deployed create logs, and these logs contain gold nuggets of information that can help defend their networks. In fact the Verizon and US Secret Service breach analysis report noted that in 86% of the breaches they investigated, the evidence of the breach was present in the log files, but in only 3% of the cases were these logs used to detect the breach.

Community banks can avoid becoming another breach statistic by employing real-time log monitoring, analysis, notification and response technology. This technology takes the network and security products they already own and makes them smarter and more effective.

TriGeo SIM is built to capture the millions of events occurring every day and provide the intelligence needed to find the security event needle in the network haystack. TriGeo empowers IT teams with both real-time analysis and response - which means that we are effective at both detection and defense. In a world where the last worm traversed the entire Internet in a matter of minutes, we know that seconds count, and that is where TriGeo's focus on analysis AND response is critical. You can think of us as an early warning system, combined with automated defenses - all of which protects your bank from the inside to the outside and vice versa.

**Michelle Dickman**  
General Manager



**Michelle Dickman** is president and chief executive officer of TriGeo Network Security. Ms. Dickman has spent over 20 years in the software and financial industries combined. Much of her extensive management, sales and marketing experience has been focused on the midsize enterprise which is TriGeo's core market. Dickman also brings considerable business development and management skills to TriGeo. As the co-founder and President of an ERP software company, Dickman grew that organization from ten to nearly one hundred employees, with four regional offices, and annual growth ranging from 20 to 60 percent. Her leadership ultimately led to the organization's acquisition by a public company.