

## *Protecting Customer Data at Rest and in Motion*

There are a whole range of threats to bank data, from malware to employees to weak security and audit controls. Unfortunately, new malware attacks are constantly being created, refined and launched, including "zero" day exploits. It is incumbent on banks to be vigilant in their patching in order to help protect against these seemingly never-ending threats.

The importance of employee security awareness training can hardly be over stressed. Ongoing staff education, combined with data leak prevention tools, is a winning combination. Of course the foundation for any bank is to have a comprehensive and integrated layered security filtering program in place. A key part of this strategy entails analyzing where critical data is stored and then taking appropriate measures to compartmentalize and protect sensitive customer information.

Other technologies that contribute to a defense in depth approach include port-based authentication and host-based IPS (intrusion prevention systems). Port-based authentication is a "network access control" concept in which a particular device is evaluated before being permitted to communicate with other devices located on the network, while host-based IPS is rapidly gaining popularity in addition to the better known network-based IPS that many banks deploy. Regardless of the number of defense layers in place, they all must be actively monitored, managed and audited. We can't over emphasize the importance of the simple concept of: test, test again, re-test!

As "trusted" and sensitive data moves from one place to another, emphasis is placed on authentication of source and destination hosts, evaluation of the data's integrity throughout, and audit controls over the entire process. Encryption of data is critical as it leaves the trusted network, but doesn't always imply greater security within the confines of a properly architected bank network. Through the use of Simpler-Webb's real-time monitoring and security alerting service, a bank has access to most records of network and security activity in a single, consolidated location.

Simpler-Webb offers comprehensive consulting and a suite of managed services that address most layers of the bank's information security infrastructure, leveraging both commercial and proprietary applications. Not a one-size-fits-all kind of company, Simpler-Webb identifies the most appropriate solution for the client's network, systems and people. We start with a baseline assessment of the bank's security posture, interview key persons to assess the business goals and how to best align with operational and financial constraints, and then propose a phased implementation of both point and systematic applications that filter out known threats and institute controls to limit the risk from unknown sources. By making these kinds of concerted efforts for the past fifteen years to be our clients' trusted information technology partner, we have earned the trust of dozens of leading financial institutions across the country and look forward to helping other banks become more secure going forward.



**Jeff Simpler**  
CEO

**Jeff Simpler** is co-founder and Chief Executive Officer of Simpler-Webb, Inc., an Austin, Texas-based corporation serving the Information Technology needs of clients for fourteen years nationwide, including hundreds of financial institutions. Jeff provides strategic direction for Simpler-Webb, establishes client relationships, and ensures the long term success of their projects. Jeff's expertise centers on networking technologies with a focus on design, integration, and management with an emphasis on network security solutions and implementation. A frequent speaker at financial institution meetings and conferences, Jeff delivers practical case analysis and application to customer environments.

**SIMPLER WEBB**  
Information Technology Solutions

**Contact Info:**

<http://www.swinc.com>