RIDING SHOTGUN

While Wells Fargo no longer uses the Pony Express to communicate with customers, it still needs to guard messages, reports Greg Masters.

When Henry Wells and William Fargo founded a company to provide banking services to Californians in 1852, their quickest means of communicating with customers was via the Butterfield Overland Mail Company, the precursor to the fabled Pony Express. When the partners acquired the western operations of the delivery service eight years later, this was the first in a series of acquisitions that over the next 150 years would absorb a number of banks.

Wells Fargo & Company is now a diversified financial services company with $1.3 trillion in assets. And it no longer relies on horses to carry messages to and from its 282,000 team members and 80-plus businesses. Headquartered in San Francisco, it operates 10,000-plus banking stores in 39 states and the District of Columbia.

Bipin Sahni , vice president, Wells Fargo Wholesale Banking group, says that because Wells Fargo must deliver confidential documents to its customers, and they need their financial informa-

Copyright Haymarket Media, Inc.

Bipin Sahni , vice president, Wells Fargo Wholesale Banking group

tion quickly for decision-making, his team was charged with finding a secure and easy-to-use method for its customers and team members to communicate by email.

Sahni heads the wholesale architecture and commercial electronic office (CEO) mobile application development team and is responsible for providing and setting the direction for the application architecture for products rendered through the CEO portal. The technology and operations group supports the company's entire hosting needs, which include application hosting, mail servers, information security and enterprise information management for all its lines of business.

He and his team considered several email encryption products and chose Voltage SecureMail. "Our first consideration was the system's ability to protect confidentiality of private information about our customers," says Sahni. "Our customers are at the center of everything we do. We make decisions from their perspective, and we protect the confidentiality of private information about them."

Ease of adoption was also a key factor. "Voltage SecureMail gives us an automated way to deliver information to customers and team members quickly and securely, wherever they are," he says.

No special software is necessary for recipients and it works seamlessly with existing email environments, says Tammy Schuring, vice president of customers, Voltage Security. "When sending an encrypted message, you simply write the message and press the 'send secure' button. No certificates, tokens or other security credentials are required."

In fact, she says, most customers configure their systems to automatically encrypt messages based on content, so they read and respond to encrypted email exactly the same as unencrypted email. The encryption is handled at the network edge automatically.

Voltage SecureMail was first deployed in the Wells Fargo's Wholesale Banking group, which serves middle-market businesses nationwide. It is now being rolled out company-wide. Sahni says that because Wells Fargo has extensive IT systems and infrastructure connected to its messaging infrastructure, his team had to ensure that all business processes were supported.

"We integrated it with our complex messaging environment, which includes archiving, content scanning and mobile infrastructure," Sahni says. In some cases, this produced innovations. For instance, being able to blind copy participants in an ongoing encrypted email keeps everyone in the loop, he explains.

While the Voltage system is centrally administered, different business groups within Wells Fargo have different requirements or policies. For example, division names on emails might differ, or different business lines might want to direct clients to different customer service numbers. "Our goal is to expand usage across the company," he says.

The system is essentially invisible to the company's team members and easy to use for customers, he says. Other factors that went into his reasoning for the purchase included the tool's low total cost of ownership, and the fact that there are no downloads, directories, certificates or duplicate systems to manage.

Another differentiator is that Voltage SecureMail does not store any information when encrypting, says Voltage Security's Schuring. Even keys are dynamically generated and do not need to be archived for disaster recovery or regulatory compliance purposes. "This

Tammy Schuring, vice president of customers, Voltage Security

IBE: Efficient encryption

Voltage SecureMail is based on a cryptography system known as identity-based encryption (IBE) – now in use at major corporations around the world, says Tammy Schuring, vice president of customers, Voltage Security. "IBE provides a simple, but secure way to handle encryption and key management, resulting in highly scalable implementations."

IBE is a public key cryptographic system that uses a recipient's email address as their public key, she explains. Access to decryption keys is governed by an organization's identity management systems, including Active Directory.

 Copyright Haymarket Media, Inc.

results in dramatically reduced costs, reduced business processes and reduced infrastructure for disaster recovery and business continuity," she says.

Updates are centrally managed by the organization. "Updates to server components can be pushed out from a central console and updates to client-side software plug-ins can be handled via any standard deployment management tool," says Schuring.

"Financial services customers have a greater understanding of security issues," she adds, "so there is no margin for trial-and-error for an email encryption provider."

Wells Fargo's Sahni was also pleased that there was little need for his team to provide support. "Without directories or certificates to manage, operational overhead is low. We've integrated the system into our pre-existing environments, which include archive, data leakage prevention, e-discovery and mobile infrastructure."

The implementation also helps ensure regulatory compliance. More than that, however, says Sahni, it's also viewed as a valued-added service that the company can provide to its customers. "Trusted and secure communications are a critical part of our customer-centric strategy," he says. ■

VOLTAGE SECURITY, located in Palo Alto, California, is an encryption innovator and global leader in end-to-end data protection. Voltage solutions, based on next generation cryptography, provide end-to-end encryption, tokenization, masking and simplified key management for protecting valuable, regulated and sensitive information based on policy. Voltage products enable reduction in PCI audit scope with rapid implementation and the lowest total cost of ownership in the industry through the use of award-winning cryptographic solutions, including Voltage Identity-Based Encryption™ (IBE) and a new breakthrough innovation: Format-Preserving Encryption™ (FPE). Offerings include Voltage SecureMail™, Voltage SecureData™, Voltage SecureFile™ and the Voltage Security Network™ (VSN), a SaaS service for the extended business network. Customers include Global 1000 companies in banking, retail, insurance, energy, healthcare and government. www.voltage.com

Voltage security

SC MAGAZINE Reprints

 Copyright Haymarket Media, Inc.