

From Manual to Optimal

Citizens Business Bank's proactive approach to security involves everyone—from the board room to the end user

In the mid-1970s, Southern California's Inland Empire region was in rapid transition from an agricultural economy to a major urban center. In that environment, business and community leaders established a new bank, with the goal of offering the best financial products and services while maintaining a level of customer service reminiscent of the area's small-town past.

Just over 30 years later, Citizens Business Bank has over \$6 billion in assets and 44 commercial banking centers in California, from Orange County to Stockton. The firm's financial strength prompted *U.S. Banker* to recognize Citizens as the nation's Top Business Bank in January 2007.



Elsa Zavala, Senior VP and CIO, Citizens Business Bank

By Vicki Powers and Mark L.S. Mullins

Through this growth, the bank has maintained its reputation for excellent customer service and, in an era of rapid employee turnover, Citizens' associates are more likely to stay on board for an extended time.

One of those long-time employees is Elsa Zavala, who joined the bank's Information Services Department in 1993, and became the CIO in 2000. At the time, the bank was launching its online banking services and expanding its Web presence, and Zavala recognized the potential dangers that came with that expansion.

"At Citizens Business Bank, information security is an issue that goes all the way to the Board of

Directors," Zavala explains. "I provide them with a quarterly report on where we stand from a security perspective, and I'm proud to say that they are personally invested in ensuring the safety of our customer data."

A proactive approach

Citizens' proactive approach to security is difficult to maintain in today's rapidly evolving landscape. "Banks are reacting to security threats and compliance requirements as they come, but they have no enterprise strategy to be more proactive and plan for what's going to be coming," says Jeanne Capachin, Research VP, Banking Practice, at Financial Insights, a Boston-area financial

technology research firm. “They can never take a step back and take a broader view, because they are always reacting to the next new thing.”

Experts suggest that security is an increasing factor in earning the trust of customers and providing a competitive differentiator to grow the business. “Banks are not the target, but they must take responsibility and ensure their customers still trust they can keep their information secure. Very often, this requires making a financial investment to react to security concerns,” Capachin relates. As a result, North American banks are expected to spend \$10.7 billion this year on new technology investment opportunities alone—most notably around security and regulatory/compliance solutions.

Bringing in the experts

Having experienced both organic growth and growth by acquisition, Citizens realized that the plethora of manual processes in use to integrate and manage security and compliance issues would quickly become unwieldy. Adding new Web-based services to this mix made new technology solutions even more necessary. “I didn’t want to increase my staff and develop their expertise for 24/7 coverage of the latest and greatest security threats,” explains Zavala. “We wanted to depend on experts to manage this for us.”

To handle its security monitoring requirements, the bank turned to Symantec Managed Security Services to monitor and manage the bank’s security infrastructure, which today includes Symantec firewalls, network intrusion detection systems, and endpoint security software.

“I didn’t want to increase my staff for 24/7 coverage of the latest and greatest security threats. We wanted to depend on experts to manage this for us.”

—Elsa Zavala, Senior VP and CIO, Citizens Business Bank

Symantec Consulting Services also provided a vulnerability assessment that helped the bank write its security policies, designing them to ensure compliance with a wide range of regulations. The initiative helped the bank prepare for FDIC audits and meet internal standards that at times are even more stringent than external regulations. “Ensuring that best practices were in place before the launch of online banking helped protect online customers during the crucial early adoption phase,” says Zavala.

Keeping the inbox clean

Unfortunately, the banking industry is no different than any other when it comes to spam. This toxic email clogs networks and crumbles productivity, forcing workers to spend time identifying and deleting unwanted email messages. It adds up: U.S. business alone lose \$70 billion a year—equivalent to \$712 per employee.

Citizens Business Bank had spam problems in spades: Nearly 75 percent of its 40,000 daily incoming emails contained spam. With 1,100 mailboxes, Citizens was losing more than \$450,000 annually in employee productivity. For the IT team specifically, dealing with spam-related issues consumed up to four hours daily.

In mid-2006, Zavala’s team migrated to Symantec Mail Security 8260 appliances.

The results were immediate: spam traffic decreased by 95 percent, from 30,000 messages a day to just 500. Deployed at the Internet gateway, the security appliance not only makes email more secure and enhances worker productivity but also creates reports on demand, documenting the number and intensity of attacks. “We sought a comprehensive anti-spam solution that would not only provide protection at the Internet gateway but also enable the team to manage email threats proactively,” says Zavala.

Tracking compliance

Technology plays a significant role in the integration of compliance requirements into existing business processes. In fact, banks maintaining between \$1 billion and \$10 billion in assets will spend \$77 million in risk management and compliance solutions in 2007, with forecasted increases to \$86 million over five years.

At Citizens, two bank employees previously spent 50 percent of their time preparing for audits and assembling compliance documentation. In 2006, Zavala’s team deployed Symantec Control Compliance Suite for the bank’s server environment, helping to lower compliance costs through automated assessment of policies against industry regulations. Control Compliance

Suite's built-in Policy Module receives this data and helps document compliance with the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, and FDIC regulations, as well as the bank's internal policies.

"This solution will have a significant impact on operational efficiency," Zavala explains. "The two employees tasked with these manual processes can now be deployed to more strategic projects in

Web training modules—at their own desktops and on their own schedule. Employees answer questions at the end of each module to test their understanding of the material. And the IT team can easily track who has completed the training, an activity that is essential for compliance tracking.

With 780 employees participating in this online training every month, awareness is increased with a wide range of

vendor relationship simplified security administration and increased the usability of the solutions. And, having a single point of contact minimized staff time, energy, and expertise required to maintain the security infrastructure.

The bottom line has benefited as well: Citizens saves more than \$400,000 per year by outsourcing security monitoring while avoiding staffing additions to manage

its devices. Today, 15 minutes a day is all it takes to manage these devices—a dramatic decrease from the estimated seven analysts it would require to manually monitor 10 devices per shift, reviewing, investigating, and responding to notifications around the clock.

Many banks have grown their security infrastructures piece by piece, always selecting best of breed—and then noticing the

inefficiencies and gaps in that approach. Citizens illustrates that developing a trusted vendor relationship upfront can improve security, streamline administration, and reduce total cost of ownership for the security infrastructure. "We pride ourselves in relationship banking, and really knowing what it takes to take that re-relationship to the next level," says Zavala. "Our experience has been the same with Symantec." ■

Vicki Powers is a freelance journalist who writes frequently about business and technology.

Mark Mullins is a member of the Symantec Customer Leverage Program and writes for Symantec.com.



Read Online:
www.symantec.com/ciodigest/americas/citizens

“At Citizens Business Bank, information security is an issue that goes all the way to the Board of Directors. I’m proud to say that they are personally invested in ensuring the safety of our customer data.”

—Elsa Zavala

the organization.” This staffing reallocation equates to an estimated \$100,000 annually in staff productivity.

Generating awareness

Security and compliance policies are meaningless unless bank employees understand their role in enforcing them. In the past, the bank conducted a single security training course every year. It was costly to assemble trainers and employees at central locations, some employees inevitably missed the training, and, in the end, employee retention of this “data dump” was not as high as hoped.

In early 2007, Citizens changed its approach to security training. Now, the bank requires employees to complete monthly online

security issues. For instance, employees now understand the importance of strong, complex passwords, and the potential risks posed by including email addresses on business cards or out-of-office messages that refer the caller to a specific person. “Employees retain much more of the training now. It has also reduced the cost and logistics needed for live training,” says Zavala.

A relationship of trust

Keeping track of multiple technology vendors plagues many organizations not working with an enterprise view. Citizens focused on choosing Symantec solutions to replace several of its existing technologies already in place. Moving from a silo-based model to a trusted