



Banking On Security

Financial services firm goes to VeriSource to secure its network

By **Cristina McEachern**, *VARBusiness*
11:00 AM EDT Mon. May. 23, 2005

It's no secret that security is of the utmost importance in the financial-services industry. And, lately, who can ignore the headlines about Bank of America's losing backup tapes with confidential financial information on 1.2 million federal employee customers, including senators, or HSBC Holdings' notifying more than 180,000 GM-branded MasterCard holders that they could be at risk for identity theft after their credit-card information might have been accessed by criminals?

The ever-mounting scrutiny on security by federal regulators and, specifically, the Office of the Comptroller of the Currency (OCC), which oversees guidelines on the security of customer information and data, is what prompted Bentonville, Ark.-based ANB Financial to beef up its infrastructure. With more than \$650 million in assets, the bank prides itself on being technologically savvy--adopting document imaging in 1994 and introducing online banking back in 1996 before the online onslaught picked up steam.

But, of course, with these types of offerings comes the opportunity for security breaches and compromised data. And then there are the regulators, particularly the OCC, which has strict guidelines for ensuring data privacy and network protections.

"We're such a heavily regulated business," says Cris Carter, vice president of electronic data processing at ANB Financial. "And right now, there is such an emphasis on data and data security, which we take very seriously."

Beefing Up the Network

More specifically, examiners from the OCC visited ANB Financial about two years ago to test the intrusion-detection system the bank had in place. Carter says that while the system was up to par, "they wanted to see even more security in that area."

So with that mandate in place and the regulators calling for more security, Carter leaned on VeriSource, a Rogers, Ark.-based solution provider that has worked with the bank quite regularly since ANB Financial opened its doors in 1994.

"Usually we sit down and have meetings, and those meetings have become much quicker as we've become more and more familiar with the bank," explains Don Goff, COO at VeriSource. Goff says that understanding the needs of the bank and its risk comfort level is an important part of the relationship.

Carter's needs? **He was looking for an intrusion-detection system that was "intelligent" and could not only monitor the network and identify problems, but also work to automatically correct problems that cropped up. The long-term goal, Goff says, was to implement a**

system that could do things like, "tell the firewall or routers or switches to take action without human intervention."

Goff got right to work researching intrusion-detection solutions and coming up with viable options for ANB Financial. An initial list of potential products was presented to ANB Financial; although he wouldn't reveal names, Carter says that VeriSource presented several alternatives--one that was a much more recognizable brand, and a couple that were more expensive but just didn't meet the bank's needs. One product that Carter had not heard of was **Enterasys Networks' Dragon solution.**

"The pricing was good, and the capabilities were very good," Carter says. So ANB decided to go with Enterasys.

"When we went out to look for this type of system, there were a few products out there, but Dragon did the majority of the things we were looking for and interacted well with the bank's existing systems, which was a huge plus," Goff says. For example, one of the options was less expensive for the hardware and software, but involved a service with a recurring cost.

"We knew the OCC was really putting stress on internal security and being able to prove you're locking down the desktop," he says.

Carter says that when it came time to make the decision, his confidence in VeriSource made him comfortable with a relatively unknown product.

"Based on their recommendation and what we'd seen, we went ahead with the Enterasys product," Carter says. "We decided to give it a go."

VeriSource deployed Enterasys Networks' solutions, including Enterasys Matrix N3, C2 and E1 switches, and XSR Security Routers. At the heart of the network is the Enterasys Dynamic Intrusion Response solution (DIR), which includes the Dragon Intrusion Detection System and NetSight, which is a suite of network-management software that includes Automated Security Manager (ASM). ASM is able to take security events from Dragon, locate the exact port on the switch where the attacks are entering the network and automatically take action on the port to stop the threat.

Carter says that the switches and intrusion-detection solution combined totaled approximately \$130,000, with the additional services, implementation and customization covered by an ongoing contract ANB has with VeriSource, which also acts as the bank's network administrator.

Carter explains that the heavy focus on data and data security stems from changes in the banking landscape during the past few years.

"The OCC comes in to examine the bank on a regular basis," Carter says. He says that Y2K and 9/11 shifted the primary focus of regulators from issues such as lending policies and making sure loans were secure to a data-security-heavy focus.

"IT has really shot up to its own level of importance," he adds.

And although Y2K proved to be a non-event, Carter says it woke up the regulators to see the vulnerabilities of the banking system beyond just making bad loans.

"As you roll out more technologically advanced methods--like Internet banking, wireless networks and all of the various communications that go on between a bank and its customers--all of that has to be protected now," Carter says.

Intrusion Detection In Action

At the bank's next exam by the OCC, the regulator brought in a regional person in addition to the local individuals who generally do the exams.

"His focus was on intrusion detection, and he started looking at Dragon skeptically, but after he got into it, he was amazed and really blown away by it," Carter says.

The letter of recommendation left by the OCC examiners pointed to the "powerful tool" ANB had in place and challenged the bank to "exploit it and make sure we're using it to the fullest capacity," Carter says.

Carter also has external auditors and others who do penetration testing and issue reports, which the OCC takes very seriously, on the strength of the bank's networks.

In terms of responding to attacks, Goff says that recently his staff was looking at ANB's intrusion-detection logs and noticed a single computer was constantly scanning the bank's network. Goff knew that was abnormal and could be a potential hacker looking for a way in, so he contacted the computer's Internet service provider (ISP) and explained what this computer was doing.

"We said this person is constantly scanning our servers, and we consider this an attack," Goff says.

The ISP then went out to the customer who was scanning and ordered him to cease and desist his actions, or face discontinuation of his service. While the scanning went away for about a week, it came back once again with the same IP address. Goff was immediately on the phone with the ISP, which decided to discontinue the person's service.

"It's so important to be able to watch for those things on a regular basis and be able to take action," Goff says. *