



# Network Protection 101

Learn what steps to take to identify and prevent breaches in internal networks

By Bridget McCrea



The first time the technology team at the Bank of Utica, N.Y., considered a security information and event management solution, the group suffered a bit of, well, “sticker shock” and put the initiative on the backburner for a few years. The team revisited the idea in 2006, the same year the Federal Financial Institutions Examination Council (FFIEC) came up with new regulations concerning the way banks track network changes, logs and other elements.

For banks to comply with the FFIEC regulations in the most effective manner, it seemed that network protection functions would have to be automated and software-driven, giving banks the ability to quickly archive and analyze data, and react as needed.

The regulations sent the single-location, \$750 million-asset Bank of Utica back to the drawing board in search of a solution. Having already reviewed TriGeo Network Security’s SIEM program a few years earlier, Jeff Smyrski, the bank’s network administrator, decided to give it a second look. “We looked at a few products (including LT Auditor, which didn’t meet the bank’s needs), got the documentation to support the investment, and presented it as something we could do as a bank,” says Smyrski. “I was able to cost-justify it, and show how it would make life simpler.”

For Bank of Utica, the SIEM solution monitors applications and programs that run on a 24-hour basis;

meets FFIEC compliance guidelines for logging user access and security events; troubleshoots new problems (such as when Internet banking applications function improperly); and notifies the bank of USB drive use on its premises. After undergoing SIEM installation and training—both of which were “a breeze,” and took about four weeks to complete, according to Smyrski—the bank has created several new rules, thus “fine tuning” the solution to meet its needs.

One such rule allows the bank to monitor processes that are being handled by its servers, which generate morning reports. When these reports are inadvertently closed, or if they don’t run at all, Smyrski is alerted immediately via an e-mail message or phone page. (In the past it sometimes took hours for Smyrski to be notified about a glitch.) The institution can also monitor the status of files that are copied (moved to a back-up location on a five-day rotation), that are at risk of being overwritten and lost forever, and that shouldn’t have been created in the first place.

## Open Arms

The fact that Bank of Utica overcame its initial “sticker shock” to invest roughly \$20,000 (an estimated software cost, according to TriGeo) in turnkey SIEM software isn’t that surprising in the financial services industry, where regulatory compliance and the prevention of network security breaches have become top-of-mind issues for banks of all sizes.

According to Paul Stamp, principle analyst at Cambridge, Mass.-based Forrester, financial institutions can “bank on” the fact that a security breach costs anywhere from \$90 to \$305 per record (the average is about \$130).

Stamp points to solutions from TriGeo, High Tower Software, eIQ Networks Inc., and RSA, the

### Key Selling Points

Michelle Dickman, president and CEO at Post Falls, Idaho-based TriGeo Network Security Inc., says her firm’s SIEM solution has been available to mid-sized financial institutions since mid-2003. One of its biggest selling points, she says, is the way in which it tracks, analyzes and reacts to security

of music players and flash drives by employees at work, based on the fact that the machines “lock down” when a non-approved gadget is inserted into a USB port. Smyrski says being able to write rules that govern that type of activity has helped the bank’s technology team be more proactive about security. “We don’t have

**“We don’t have to wait until there’s a problem. We can just state that if certain things happen, then the system must take a specific action.” – Jeff Smyrski, Bank of Utica**

security division of EMC, as the ranking popular choices for banks looking for security information and event management solutions. He says the total cost of ownership for these programs comprises four steps:

- Purchasing the solution;
- Getting it up and running;
- Expanding the bank’s infrastructure to include the solution; and
- Responding to the information that’s generated by the system.

The best systems, according to Stamp, are able to identify those risks that banks must respond to and prioritize them in a way that allows the institution to make the best use of its time and resources. The systems should also streamline the actual response process by, for example, answering queries like, “Tell me everything that Bob Johnson did between the hours of 2 p.m. and 6 p.m. last Saturday.” Reports should also be streamlined, and available to bank employees—and auditors—on an ongoing basis.

breaches in real time. “We are literally next to the events when they occur,” says Dickman. Should an unauthorized individual attempt to log onto the network and hit a firewall, for example, the system can be disabled instantly.

With regulatory compliance as a top benefit of his bank’s security information and event management system, Smyrski says his job has been simplified by those “instant” alerts and lockouts, the latter of which he typically learns of before the user even knows he has been identified as a potential threat. “I get a page or an e-mail, and then I just wait to hear the phone ring,” says Smyrski. Recalling a time recently when an outsourced auditing firm was completing an internal scan, he says, “Our security system was going crazy, popping like mad on one machine after another, as if someone was trying to log onto a critical account. We were pleased to see that.”

A utility known as USB Defender has helped the bank cut down on unauthorized use

to wait until there’s a problem,” he says. “We can just state that if certain things happen, then the system must take a specific action immediately.”

### Learn More

Read “Responding to a Card Data Security Breach: Practical Steps for Protecting Your Card Base and Your Reputation,” at [www.nyce.net/resources/pdf/Responding-toDataSecurityBreach041206.pdf](http://www.nyce.net/resources/pdf/Responding-toDataSecurityBreach041206.pdf).

Stamp says he expects more institutions to take similar approaches for regulatory compliance to identify and prevent breaches of their own internal networks and identify exactly who has accessed those networks in the last 24 hours. “What was once the domain of the [the biggest financial institutions] is now working its way downstream, particularly in the mid-market.”

**ib**

*Bridget McCrea is a free-lance writer in Dunedin, Fla.*