

SC

MAGAZINE

FOR IT SECURITY PROFESSIONALS

REVIEWED IN THIS ISSUE

Aventail ST2 P75
SSL VPN device for large networks that require a lot of power



Solsoft P71
Policy management with logical automation and reports



AirMagnet P68
Protects wireless LANs with hardware-based sensors



FEATURES:

Protecting Wall Street

Sunil Seshadri on how the NYSE protects its data **P26**

Digging for dirt

Enterprises need to have forensic systems in place after a breach **P32**

Safe at rest

With insider threats, security is turning toward stored data **P36**

GROUP TESTS

» Policy management

Tools reduce complexity of company networks **P66**

» SSL VPN

Easy to deploy, simple to use, browser-based devices **P72**





The NYSE Group's Sunil Seshadri, vice president of information security, IT risk management and compliance; and Steve Rubinow, chief technology officer.

Photos by Jordan Hollender

“Let’s trust, but let’s verify and monitor that process.”
— Sunil Seshadri, vice president of information security, IT risk management and compliance, NYSE Group

When Sunil Seshadri discusses the security philosophy at the New York Stock Exchange (NYSE), inevitably conversation drifts back to the importance of data-centric security.

“At the end of the day everybody looks at what the business dependency is on data that we have,” says Seshadri, vice president of information security, IT risk management and compliance for NYSE Group. “Historically, with organizations there has been a tremendous amount of focus on securing the perimeter — keeping the bad guys out. But at the end of the day, what is it they’re trying to reach? They’re trying to reach some set of confidential or sensitive data at the backend.”

Like many in extremely sensitive or regulated environments, Seshadri believes that a network-centric security stance is not enough to protect the integrity of valuable data. Sure, network and perimeter security measures can do a lot to protect against external malfeasance or breaches, but what about users already inside? He believes that one of the best ways to ensure application-level data retains its integrity is to appropri-

ately control, monitor and log access to the targeted data, specifically at the database and system levels. NYSE, then, leans more toward data-centric security policies in order to maintain the integrity of the data that it most relies on.

“In my profession, it is not that I don’t trust people — but I don’t,” Seshadri says. “If there is a philosophy that I adopt, it is ‘Let’s trust, but let’s verify and monitor that process.’”

At NYSE, there are hundreds of millions of transactions that pass through company systems each trading day. The well-being of hundreds of corporations, and the economy as a whole, depend on the integrity of this transaction data, which is why Seshadri and his team have taken pains to ensure they know exactly who has access to this data and what they are doing with it in real time.

Currently, Seshadri uses database auditing to keep track of electronic trading facilitated by the NYSE Arca division, which was formed as a result of the NYSE-Archipelago Holdings merger earlier this year. Before the deal, Archipelago was completely *Sarbanes-*

The New York Stock Exchange takes a data-centric approach to secure its valuable asset — trade data, reports [Ericka Chickowski](#).

PROTECTING

WALL STREET

Data lifecycle management

Oxley (SOX) 404 compliant through the use of the auditing tools and other oversight measures. He plans to bring the same tools to the floor trading databases of the NYSE Group by the end of 2007 in order to meet the newly formed company's deadline for SOX compliance.

This kind of oversight is critical in lines of business such as those at the stock exchange, where the temptation for an employee to go rogue can be extremely high. According to Ellen Libenson of Symark, an identity management and access control vendor, simply putting the tools for accountability in place can be a powerful deterrent.

"Everybody is human, everyone is subject to temptation at some point in their [lives]," she says. "And if you have a fox in the henhouse, it'd be nice to never find that out the hard way. If everybody's access is documented and they know there is accountability, then they are less likely to cross that line."

According to Seshadri, the monitoring activity is as important as the access management issues. "For a lot of companies it comes down to 'Do the right people have access to their information?'" he says. "I think they are able to answer that from an entitlement standpoint, but the question then becomes, 'Are these right people doing the right things?'"

Seshadri and his security team rely on



At the end of the day, everybody asks what is the business dependency on data..."

— **Sunil Seshadri**, vice president of information security, IT risk management and compliance, NYSE Group

database auditing tools to make certain that privileged users don't abuse their rights. "When someone like a database administrator makes a change — be it to a database structure, a schema, a trigger or a value in a table — all of that is actively recorded," he says.

The information security department is kept up to date on these changes through a continuous reporting structure and, in the event of a violation or problem, through an email alert that is sent only a few seconds after the event occurs. To ensure accountability, there is also a process for logging program change management — all of which

It also had to begin to formulate how the company would approach security. According to Rubinow it has been a matter of meshing two distinct policies into something that was cohesive, affordable and compliant with SOX and other regulations.

"It's fair to say that Arca had one security model and New York had a different security model — neither good nor bad, just different," Rubinow says. "And when we put the two of them together, just like with the technology strategy, we had to say 'What are the best aspects of both security models?' and then overlay cost considerations."

— *Erica Chickowski*

flows through Seshadri's department.

"We have a process with the folks on the backend where when they make a change to a program, they tie into a specific change management work order process so that there is an independent group — the information security group — that now has a line outside into the changes that are happening to financial information," he says.

The key to all of this financial data tracking and alerting comes down to a good policy that lays out the hierarchy of data and what to keep closest tabs on.

"You set up roles and rules based on the type of data, who can access it and what can they do," says Cliff Pollan, CEO of Lumigent, which is the vendor NYSE uses for database auditing.

Strong policies will lay the foundation for a strong overall data-centric security stance, Pollan says. He explains that tracking privileged users through the database is the first step to securing the data. But practitioners will likely need other point solutions to handle problems that can happen once users move beyond those applications — for example, if a user cuts and pastes information from the database, they'll need content filtering to track the data once it leaves the database.

"Often people are constraining access to the data through the application, so the reason that they're more concerned about direct access or more privileged access is that they are getting comfortable with the fact that it is a different problem once you force everyone through the application," he explains.

At that point it could become a content leakage problem, he says, which will need to be monitored by complementary tools.

Ken Davis of Oakley Networks agrees. "You have to simultaneously approach the problem from the other side. How do you monitor the behavior of those users while they're accessing that information and those resources, and then have policies in place that identify when

NYSE & ARCHIPELAGO: Security + business

One of the biggest merger announcements to hit Wall Street was the one involving the New York Stock Exchange and Archipelago Holdings. When the deal went final in March of this year, the newly formed NYSE Group began transitioning technology executives — including Sunil Seshadri, vice president of information security, IT risk management and compliance, and chief technology officer Steve Rubinow — from Archipelago over to the new business.

NETWORK SECURITY: Pioneering efforts

As the vice president and chief scientist at Verdasy's, Dr. Dan Geer has become an ardent supporter of what many call data-centric security.

To hear more of this podcast, visit www.scmagazine.com/us/podcasts.

Why should enterprises adopt data-centric security principles?

The answer is, by and large, the data. It is the data that has value, not the machinery.

But what about network security?

Authentication and network security cannot be expected to go any farther. We've put enough investment there.

Is today's enterprise ready to embrace the data-centric security model?

I think they're ready even though they don't know it. Every time someone has an embarrassing event, they are ready as of the day before. All good ideas look obvious in retrospect.

The value of the machinery is not nearly as valuable as the data itself. If you think data security is difficult or expensive, try the alternative. Try data insecurity and see what happens to you.

What is impeding enterprises?

What's impeding them is a sense of helplessness. We've had a customer say, "I don't want to know how my data is leaking, because then I'd have to take action and I don't have the facilities to do that."

There's an old joke in engineering along the lines of: "Never test for an error condition that you can't handle." It is almost the same thing here. What's changed is that in the last year the public awareness around this has gotten to the point where not doing something looks stupider than doing something. And there are now tools that you can use that actually make a difference.

— *Ericka Chickowski*



Everyone is subject to temptation at some point in life."

— **Ellen Libenson**, vice president of product management, Symark Software

that access is inappropriate, and then do something about it?" says Davis.

Oakley specializes in behavior analysis and monitoring, which can help a business check to see if a user is doing something like cutting and pasting from a sensitive application into a less sensitive spot, or doing a print screen when sensitive information is on the monitor. These types of activities can't be solely monitored by database monitoring. Separately, products such as those made by Lumigent and Oakley can be useful, but together they can be extremely empowering to an information security professional.

"There are the downstream pieces that this needs to fit into," Pollan says. "As it gets further away from the database, there are other technologies you start to use. The reason people care about where it starts, is because that's where the asset is. You should be able to say, 'We know where it started, it is in a payload somewhere in the network,' and then watch that payload as it goes through the network."

Seshadri at NYSE concurs, pointing out that the best practice is a layered, but focused, approach. For his organization, this means not only using the best data-centric techniques, but also keeping the good elements of a network-centric approach. In effect, his organization takes an inside-out line of defense, starting where the data is most vulnerable and moving outward.



"We're looking for a model that is a happy medium between a data-centric and a network-centric security model," he says.

Clearly, the New York Stock Exchange by necessity is ahead of the security curve. Though analysts, as a result of regulations such as *Sarbanes-Oxley*, are predicting a shift toward a more data-centric approach to data security, there is still a way to go before the average organization moves beyond securing just the underlying IT infrastructure.

"I think people are waking up to the fact that there has to be a sustainable mechanism in place to monitor the who, when, what, where, how," Seshadri says. "Who is accessing sensitive information? When are they accessing it? What is it that they are accessing? Where from? And how are they doing it? And do we have an appropriate controlled structure to answer those questions, be it internal to the company or any other regulatory agencies on the outside?"

By answering those questions, either through third-party tools or homegrown solutions, business will not only get a handle on data security, they'll also likely improve their operations.

"Not only does it prevent outright fraud and theft of data, I think, in general, it just helps someone run their company better," Libenson says. "You can prove who is doing what. If you log and track, you can easily go back and find out where a mistake was made." ■