QUALYS
SECURITY ON-DEMAND

CASE STUDY: New York Board of Trade – Maintaining Business Continuity

Company
The New York Board of Trade (NYBOT)
39 Broadway, 3rd Floor
New York, NY 10006

Company Profile
World's largest commodity futures and options trading exchange. The exchange is headquartered in New York, with about 210 employees and an information technology staff of 30.

Business Objective
Continuously assess the state of network security and implement controls to minimize risk of interruption to trading

NYBOT New York Board of Trade®

The New York Board of Trade (NYBOT) is the world's largest commodities exchange for "softs"—coffee, sugar, cocoa, cotton and Frozen Concentrated Orange Juice. About 21 million contracts of these global commodity staples trade annually through NYBOT, which was founded as the New York Cotton Exchange in 1870, and the Coffee, Sugar & Cocoa Exchange in 1882. NYBOT also facilitates trades in foreign currencies and derivative indices for equities. Customers of this not-for-profit membership organization include every segment of the underlying industries served by NYBOT markets, plus futures commission merchants, floor brokers, floor traders and managed futures funds.

Trading is the most important NYBOT business activity, so business continuity and preparedness are vital. For example, NYBOT was headquartered at the 4 World Trade Center on September 11, 2001—and was the only exchange in the world that had a backup trading floor at that time. Today, NYBOT is the only exchange in the world that triangulates IT operations with three sites housing pairs of separate and distinct systems to back each other up.

In Spring 2002, financial auditors suggested NYBOT consider creating a new position in the company—a Chief Information Security Officer (CISO)—to standardize and accelerate protective measures for information security. The finding determined that a growing surge of vulnerabilities in networks and other information technology potentially threatened the continuity of NYBOT operations. NYBOT hired Jim DiDominicus as its first CISO in June 2002. His charter was to quickly assess the state of digital security and implement controls to minimize risk of interruption to trading. DiDominicus immediately launched a weekly security audit of NYBOT's network perimeter. This allowed him to regularly and consistently monitor NYBOT's network security, strengthen settings in routers and take protective measures with other infrastructure. He did this without having to build a vulnerability management infrastucture or hire extra security staff to run the operation.

Technology Case
NYBOT had choices for the security audit and improvement project. The traditional option would be hiring a senior security operations staffer to conduct audits internally by hand and with open source solutions. The other choice was to outsource security audits, either to consultants doing traditional penetration testing or to a service company providing automated solutions over the web. He opted for a web service solution because

implementation was immediate, more comprehensive than a homegrown solution, and much less expensive.

"I've used open source solutions like Nessus, but they require a lot of care and feeding," he says. "I needed basic, centralized security functions running quickly." DiDominicus liked the idea of a third party provider hosting the entire solution—it shifted the burden of operations elsewhere and would serve as an outside validation of efforts by NYBOT to bolster network security and protect trading operations.

The network security web service selected by NYBOT was QualysGuard. No special software or hardware was required to use the hosted service. NYBOT controlled the web service with a standard web browser. Scans could be scheduled or done on-demand. The web service included daily updates to a database of more than 3,200 vulnerabilities, and the ability to get an enterprise-wide view of network security.

> "The Qualys web service lets me focus on the internal activities knowing that the perimeter of my network is in good shape."

Web Service Advantage

Using a web service is the key differentiator in NYBOT's story. Many organizations try to solve business problems by habit, assuming the best network and information technology solutions are homegrown or self-operated. In NYBOT's case, the complete solution was outsourced—not to a consultant, but to a trusted, turnkey service that worked on demand.

DiDominicus notes the web service is completely automated so its technology is always up-to-date, does not test security issues like social engineering, and frees up the time of his security staff. "It's like having a couple of guys do scans as often as you want." NYBOT runs weekly scans on the entire network with others done on an on-demand basis. "The Qualys web service lets me focus on the internal activities knowing that the perimeter of my network is in good shape."

"All it took was a phone call and less than an hour to get up and running," DiDominicus says. "Implementation was amazingly easy. And the results were immediate."

"We assess our state of security with reports from the web service," says DiDominicus, "and the report formats are better than anything I have seen." He says the results were easy to share with those responsible for maintaining the systems. The issue of vulnerabilities was a little foreign to IT staff, some of whom believed that firewalls, service packs and renaming administrator accounts was enough. According to DiDominicus, "seeing the weekly scan results opened their eyes a little to the pace of the vulnerability patch cycle."

NYBOT uses the security audit web service to magnify efforts by the network and IT staff. Data provided by the web service allows staff to focus on the most important tasks instead of chasing the usual false positive monitoring alerts. For DiDominicus, "It's like having a security group at my disposal."

Cost and Benefits

NYBOT uses the QualysGuard web service to monitor eight Internet-facing IPs. The web service network security audit solution provides NYBOT with a 10-to-1 payback, according to DiDominicus. Homegrown solutions would require him to hire at least one senior security technician at $85-90K per year salary, plus benefits and facilities costs. "The return is instant, it was a no-brainer," he says. "I've got it to the point where (unless remediation is required) I spend 15 minutes a week to review reports from security scans."

For a small cost and virtually no human overhead, NYBOT uses the security audit web service to ensure continuity of trading operations, and that trades are done securely without breaches of confidential information. The web service also serves as a third-party validation of NYBOT's security protection activities, which was another attraction for its executives and financial auditors.