National Theatre

NATIONAL THEATRE: PCI COMPLIANCE TAKES THE STAGE

To manage the security of its IT systems effectively, maintain PCI compliance, and cut outside consulting fees, the National Theatre wrote itself a new security script.

" The reporting functionality provides all of the detail that the technical staff needs, as well as comprehensive summaries that we need to send to our bank."

IT security manager at the
UK-based National Theatre

When one thinks of theatre, live performances, musicals, Shakespeare, and drama are certain to come to mind – surely not IT security. But for Richard Bevan, IT security manager at the UK-based National Theatre, security always is top of mind. To keep the business – and the performances – running, the theatre relies on about 60 servers, 1,000 networked workstations, and hosts and manages its own Web site that processes more than $20 million in ticket sales annually.

While most every company that process online credit card payments must comply with the Payment Card Industry Data Security Standard (PCI DSS), the National Theatre also must adhere to numerous other privacy regulations that include data about its employees and customers such as name, address, listings of disabilities, among other data points. "We have many regulations, from the UK and the European Union that mandate the proper processing and protecting of personal information," Bevan says. "It's also about doing the right thing, and protecting the information we manage," he adds.

The Need for Strong Vulnerability Management

One of the surest ways to protect that information is by making certain that servers and desktops are free of the application vulnerabilities and system misconfigurations that make breaches possible. Consider the findings of Verizon's 2008 Data Breach Investigations Report, which studied four years of forensics data on more than 500 security incidents. The report revealed that the "overwhelming majority" of attacks that exploited known vulnerabilities did so through security holes for which a patch had been available for months. "This strongly suggests that a patch deployment strategy focusing on coverage and consistency is far more effective at preventing data breaches than "fire drills" attempting to patch particular systems as soon as patches are released," the report stated.

Perhaps that's why one of the criteria of PCI DSS, which is a comprehensive security standard that establishes common processes for handling, processing, storing, and transmitting credit card data, includes the continuous maintenance of a vulnerability management program.

For the National Theatre's vulnerability management efforts, Bevan and his team had been using a number of commercial and open source vulnerability scanners, as well as external auditors, to conduct its PCI compliance assessments and conduct penetration tests. "Our internal teams were using a number of tools for our internal scans and we hired an external security consulting company that would perform our quarterly PCI scans and annual penetration test," Bevan explains.

Yet, the National Theatre found that it needed more ease-of-use and consistency from its internal vulnerability assessments. It also had to reduce the costs associated with hiring outside consultants. "Hiring external assessors was expensive and not very convenient," Bevan says. "And we found the tools we were using in-house required too much manual hand-holding. Plus, the reporting capabilities were severely lacking."

To compound those challenges, the National Theatre's entire IT staff consists of twelve full-time employees, with two administrators who are responsible for performing security functions – but neither is dedicated fully to security. "We all have many hats to wear, and not

everyone is dedicated to IT," he explains. It became clear: to effectively manage the security posture of all servers and workstations, the National Theatre needed a solution that would help to streamline its vulnerability management, protect customer and employee information, and maintain PCI DSS compliance.

Toward Automated Vulnerability Assessments and PCI Compliance

After a careful evaluation, the National Theatre chose QualysGuard from Qualys Inc. QualysGuard, delivered as an on-demand service over the Web, simplifies the typical time-consuming deployment, maintenance, and updating of vulnerability management servers and software. Using an efficient and cost-effective Software as a Service (SaaS) approach, QualysGuard delivers industry-leading vulnerability management and comprehensive IT policy compliance as a simple, fully turnkey service. For the National Theatre, QualysGuard automates the process of vulnerability management and policy compliance across its network, including network discovery, detailed mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking.

Because Qualys is an approved PCI scanner vendor, the National Theatre relies on QualysGuard to maintain continuous PCI DSS compliance. In fact, the National Theatre uses QualysGuard to complete all of its validation requirements. Using QualysGuard PCI, Bevan easily can complete and submit the PCI self-assessment questionnaire online, and perform predefined PCI scans on all relevant systems to identify and resolve network and system vulnerabilities. "The reporting functionality provides all of the detail that the technical staff needs, as well as comprehensive summaries that we need to send to our bank," Bevan says.

QualysGuard is much more than just a vulnerability scanner. It also keeps us up to date with what's going on out there and new vulnerabilities that arise, and it helps us to manage our networked assets more effectively," he says.

Increasingly, that also includes the National Theatre's Web applications as well as its growing number of virtual systems. Because QualysGuard has the ability to identify virtual hosts and map virtual systems, Bevan explains how this assures him that the IT team doesn't miss any so-called "rogue" virtual systems that may be deployed. "QualysGuard not only helps us recognize virtual servers and vulnerabilities, but also vulnerabilities that may be in the VMware operating system," he adds.

As a result of the recent change in PCI DSS 6.6, which requires Web applications to be secured, Bevan also is using QualyGuard's Web application scanning module to evaluate the organization's custom-built Web ticketing applications. "This is a great feature in QualysGuard that we're just starting to use, and it helps us fulfill the new Web application PCI requirements," he says.

The National Theatre has met all of its goals from its QualysGuard deployment: to streamline its vulnerability and PCI DSS compliance management and cut the costs of outside consultancies for all of its quarterly scans. "When you examine the amount of man hours QualysGuard saves us in our own manual scans and the cost of hiring external third-parties, the ROI is clear," says Bevan. "Most importantly, it help us improve our security."

OVERVIEW
Headquarters: London, United Kingdom
Business: Produces plays in its three theatres -- the Olivier, Lyttelton, and the Cottesloe – and a programme of platform performances, outdoor events, exhibitions, backstage tours throughout the year.
Size: 900 employees

BUSINESS PROBLEM
The National Theatre needed to streamline the way secures its infrastructure, and maintain compliance to the rigorous PCI DSS.

OPERATIONAL CHALLENGE
The National Theatre wanted a vulnerability assessment solution that was more accurate, easier to use, and provide better support for PCI DSS compliance, while also reducing its dependence on outside consultancies.

SOLUTION
QualysGuard

WEB SITE
www.nationaltheatre.org.uk

ON DEMAND SECURITY