



## Building a secure future: lessons learned from 2007's highest-profile security events

By Vijay Basani

**Between the proliferation of worms, Trojans and botnets, and the outbreaks of cyber attacks, 2007 was a daunting year for even the most hardened IT security professional.**

Clearly the most worrisome event, however, was the surge of targeted attacks and identity theft, which was best exemplified by the high-profile TJX Companies' security breach. While many details about the TJX breach have not been released, what is known is that hackers penetrated a wireless connection, gained access to a server holding sensitive data, installed rogue applications and stole over 90 million customer records from a central database. And, like many large-scale breaches, the operation was carried out over a period of several months.

Given that the financial gain possible with such identity and personal data theft is substantial, we should expect attacks of this sort to be one of the most troublesome areas for enterprise IT departments moving forward. So, what lessons can be learned from the attacks that occurred over the last year? And how can organizations more effectively mitigate these potentially catastrophic crimes moving forward?

First, recent high-profile security breaches suggest that companies assume their log-based security information management (SIM) solutions will help detect and identify all breaches. Unfortunately, this is often not the case and results in a false sense of security, especially when facing TJX-like "low and slow" targeted attacks that touch different parts of the network over an extended period of time.

Close examination of these breaches suggests companies should apply three basic guidelines for preventing catastrophic breaches, which can lead to lawsuits, financial loss and damage to brand reputation.

### **Guideline one: collect and analyze more than just log data**

Analyzing log data is certainly a good place to start, but the problem is that most log management solutions focus solely on event logs, which do not contain all relevant security-related data.

For example, log files typically do not contain information about new accounts created, new users added, configurations changed, sensitive data accessed, new applications installed or new processes started. Nor does log data give you the ability to detect unauthorized access to application or system resources. After analyzing the breaches of 2007, it is clear that examining log data is not enough. Organizations also need to collect other key, more comprehensive information and analyze it for possible correlation with log data to more effectively predict threat patterns. Examples of such key information are vulnerability, configuration, asset, performance and network behavioral anomaly (NBA) data.

#### **Guideline two: collect and correlate data over months, not days**

Another lesson learned from recent breaches arises from the fact that targeted attacks often occur over weeks or even months. Many of the current SIM products that only analyze recent data are stymied by slow-evolving breaches. Short collection and analysis periods make it impossible to establish normal behavior, and thus, proactively detect anomalous behavior.

ous behavior. Data collection needs to span several months, not days, so that data correlation—across all data types and over time—can reveal targeted, slowly evolving identity attacks. Thus, to be effective, data collection and correlation must be “broad and deep”: broad in type and deep duration.

#### **Guideline three: automatically correlate multi-source data**

Now that it has been established that organizations must collect and correlate all security data—log, vulnerability, configuration, asset, performance and NBA—over several months, the third guideline pertains to data processing. Analysts working in a Security Operations Center (SOC) that uses multiple point solutions have to manually analyze data from numerous, separate IT silos—a time-consuming, inefficient and ineffective method that results in most important incidents going undetected. IT departments need to take a different approach to data analysis, with systems that enable automatic correlation and analysis of all relevant security data in real time across the entire enterprise.

### **Short collection and analysis periods make it impossible to establish normal behavior, and thus, proactively detect anomalous behavior.**

#### **A new approach to security, risk & audit management**

In the combination of these three guidelines lies the essence of a new approach to security, risk and audit management. Revolutionary? No. Evolutionary? Yes, and it is similar to how network systems management frameworks, such as HP OpenView, IBM Tivoli, and CA Unicenter evolved to help large network operations teams reduce management complexity and improve operational efficiency. Now, in the world of security, enterprises must consider platforms that integrate security, risk and audit management capabilities, and provide a single unified data management and correlation engine for processing information from multiple data silos.

While this all sounds very futuristic, this solution category has already emerged and is being

leveraged by Global 2000 enterprises. Designed to complement existing point technologies, these integrated platforms provide broad, deep and automated data correlation and the ability to immediately detect suspicious activity, rapidly analyze root causes and proactively remediate problems.

Once SOC and networks operation center (NOC) teams identify a breach using an integrated platform like this, they can use built-in tools to collaborate with each other and quickly understand the “what”, “when”, “where”, “why” and “how” of any breach. With the consolidation of multiple data silos, users are provided with the complete context of any event in a single pane, thus avoiding the “swivel chair” approach. This reduces the time to detect, understand and mitigate a breach to seconds or minutes instead of days and months, which is often already too late.

In addition to security breaches, the demands of evolving compliance regulations continue to challenge organizations. These new integrated platforms also address the rigid IT requirements of regulatory mandates and best practice policies. Organizations can identify all necessary information around compliance violations, with continuous self-assessment that eliminates the worry over audit reviews mandated by regulations such as PCI DSS, SOX, FISMA, HIPAA, GLBA and more.

Many IT security experts predict that the record-setting security challenges of 2007 will only get worse in 2008 and beyond. However, there are few better teachers than past security breaches. With the emergence of integrated security, risk and audit management platforms, organizations will be better equipped to rapidly detect and respond to security incidents, while supporting regulations and best practice implementations—laying the foundation to help ensure they avoid becoming part of future targeted attacks.

**While disparate log, vulnerability, configuration, asset, performance and network behavioral anomaly solutions can be used, the volumes of data collected creates individual silos.**

### The point solution approach

It is worth taking a moment to discuss a position that some would argue, and that is that the collection of all relevant security data can be accomplished with multiple point solutions.

While disparate log, vulnerability, configuration, asset, performance and network behavioral anomaly solutions can be used, the volumes of data collected creates individual silos.

This multiple-silo approach introduces a number of business challenges including the following:

- Cost: increases both deployment expenses because each point solution requires its own expert.

- Management: results in multiple data repositories that need to be continually correlated and managed.
- Analysis: requires the manual connection of dots to identify patterns and anomalies - this can add weeks, months or years to the time it takes to determine incident root cause.

The end result of such a cobbled together approach presents a tactical solution that increases management complexity and cost while failing to proactively and promptly identify security breaches.

Fortunately and as indicated by research from various industry analysts, IT departments are moving towards a more cost-effective, single solution approach that integrates all relevant security data to facilitate early breach detection and mitigation.

Vijay Basani is CEO & Co-Founder of eIQnetworks. Prior to starting eIQnetworks, he founded both AppIQ, Inc., an application storage resource management provider acquired by Hewlett Packard in October 2005, and WebManage Technologies, Inc., a policy driven content delivery solution provider acquired by Network Appliance, Inc. in August 2000. His experience also includes numerous senior executive positions in the financial industry at Spencer Trask Securities and Josephthal Lyon & Ross, Inc. Vijay, the co-owner of five patents for the architecture and design of the WebManage Content Delivery system, Adaptive Policy Engine and SLA Management, holds a Bachelor of Engineering in electronics and instrumentation as well as MBA and Post MBA degrees from Baruch College in New York.



[www.net-security.org](http://www.net-security.org)  
Get up-to-date security information now.