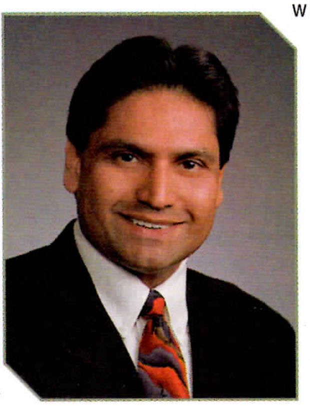
Managing the Audit Trail: The Foundation for a Legal Offensive

By Lane F. Cooper
The Washington Bureau

If companies don't take ownership of protecting their data assets and prosecuting those who threaten them, it is very likely that no one else will. That's because, according to industry analysts, "cybercriminals" have little to fear from law enforcement.



A 2001 CSI/FBI study indicates that up to 85 percent of businesses suffer computer security breaches each year and those breaches, according to another study by Exodus Communications, account for over $200 billion in annual losses. And yet, law enforcement funding for cybercrime investigation in the United States only covers about 300 federal agents—less than 0.1 percent of the 600,000 law enforcement agents serving the United States.

"People and businesses on the Internet must be responsible for their own electronic security, just as they are now largely responsible for the security of their homes [and businesses]. They must watch their transaction records with hawk-like vision," says Gartner Vice President Richard Hunter.

For most transaction-intensive companies, that creates a need for a busy hawk indeed. The problem of most corporations is not the absence of data on potential threats; the strategic challenge lies in developing a way to effectively sort through thousands of pieces of information to create a coherent picture of a company's exposure to credible threats.

"In traditional auditing paradigms, security and systems administrators have to check all of the logs from all of the servers and workstations to find out where and how problems occurred. If an enterprise network is knocked out of commission, this process is extremely time-consuming and can cost hundreds of thousands of dollars per day in system down time and lost productivity," says Umesh Verma, Chief Executive Officer of Blue Lance, Inc., a Houston-based developer of security software for Windows NT and NT/Novell networks.

Unfortunately, IT security managers frequently do not have the time or resources to engage in these kinds of investigations with traditional auditing methodologies.

But there are technologies now available that pull together the logs from all of the enterprise servers and workstations into one central repository, where it can be appropriately filtered and queried for specific patterns and user behaviors.

An audit trail can be created and used to quickly investigate what has occurred. This accomplishes several important things: the company is able to get back on line quickly; alerts are created for similar behavior in the future; and a basis is established for investigating users that could be causing problems. Indeed, the audit trail provides the foundation for taking all corrective action—whether it be legal or administrative.

> "The fact of the matter is you cannot effectively investigate and prosecute without an audit trail. Most people don't prosecute because the evidence is incomplete or it takes too long to gather it manually from across the enterprise. And once a criminal knows that you do not prosecute, they will come back over and over again."
>
> — Umesh Verma, Chief Executive Officer, Blue Lance, Inc.

"The fact of the matter is you cannot effectively investigate and prosecute without an audit trail," says Verma. "Most people don't prosecute because the evidence is incomplete or it takes too long to gather it manually from across the enterprise. And once a criminal knows that you do not prosecute, they will come back over and over again."

To ensure the security of their networks, organizations need a robust network security and audit capability. Blue Lance, Inc. (www.bluelance.com) has developed a comprehensive approach that monitors all user activity and sends out immediate alerts—sent out system-wide or to selected users. Blue Lance's solution, LT Auditor+, also brings all audit data from all applications into a single repository. The Blue Lance LT Auditor+ consolidates Windows NT and Novell NetWare log files into a server for tracking and analysis. LT Auditor+ generates enterprise-level and application-specific reports using ready-made templates or report formats that users can create themselves. The list of LT Auditor+ customers consists of financial and banking institutions including six of the 12 U.S. Federal Reserve banks, government agencies, hospitals, universities, and a number of the Fortune companies

Legal and enforcement issues raise interesting questions with regard to the audit trail. Many companies face a dilemma over whether or not to use software that actively stops specific activity hard in its tracks, or going with a passive "honey-pot" approach that allows a perpetrator to engage in illicit activity, so that a full record can be captured.

One of the key benefits of a properly managed passive monitoring approach, coupled with real-time alerts, is that corporate security officers are able to establish a clear pattern of behavior by specific individuals, while also building a body of evidence for prosecution if the damage is significant. This data pattern can then be used to create alerts as a preventative measure against future threats.

For more information on "Managing the Audit Trail," visit www.bluelance.com. ‹‹