

# Protecting Computer- Managed Assets:

**Building a Secure Infrastructure for Business**



*This report was prepared by  
the Washington Bureau of  
Larstan Business Reports,  
an independent editorial firm  
based in Washington, D.C.*

Copyright © 2002  
All rights reserved

# Protecting Computer-Managed Assets: Building a Secure Infrastructure for Business

Executive Summary .....	3
The Statistical Reality of Computer Security Breaches.....	4
Trends in Security Spending .....	4
Assessing the Cost of Infrastructure Attacks .....	5
Tackling The Threat Within .....	6
Securing the Enterprise from the Inside Out.....	6
Pairing Policy with Technology .....	7
Implementation Analysis .....	9
About the Sponsor: Blue Lance .....	10

**Editor**  
Lane F. Cooper

**Research Analyst**  
Felix Gorrio

**Protecting Computer-Managed Assets:  
Building a Secure Infrastructure for Business**

**Executive Summary**

A full 85 percent of companies in the United States experience security breaches that result in over \$200 billion in losses, according to the Computer Security Institute and the FBI. Experts say this trend saps both the financial strength and confidence of companies victimized by these attacks. Any hopes that corporate American executives ever had about finding a silver bullet that prevents 100 percent of attacks from penetrating corporate defenses have been dashed. Consequently, we are seeing a growing appreciation among C-level executives about both the internal and external threats to Computer-Managed Assets (CMA) that underpin all major enterprises.

Nevertheless, this White Paper contends that there is still a lack of senior executive involvement in and understanding of the role that “behavior monitoring-based” security strategies can play to significantly mitigate the risk of threats to CMA that can bring an enterprise to its knees.

This report explores the nature of the threats facing executives tasked with CMA protection, and discusses ways that the risks associated with those threats can be managed and mitigated. It calls for executives in both the public and private sector to take a strategic approach to comprehensively monitor and audit behavior on enterprise systems so that effective alerts and alarms are directed to the corporate security and system administration staffs.

To that end, this report provides a brief overview of the five basic steps organizations can take to initiate a proactive strategy that cost-effectively manages the threats described.

## **The Statistical Reality of Computer Security Breaches**

The staggering accumulation of value found on the enterprise systems of a typical corporation—in the form of vital content such as intellectual property, customer information, financial assets, or any other type of confidential data—underscores the risks and challenges corporate executives charged with information assurance face everyday.

“These assets are mainly information that historically would have been maintained in physical files,” says Mark Altman, Director of Altman Technologies Ltd, an information technology distributor based in the United Kingdom. “This covers correspondence, agreements, quotes, invoices, purchases, budgets, revenue/profit/accounting data, salary/payroll, personnel details, competitive analysis reports...the list goes on. All of these assets need to be accessed by the appropriate people only.”

Protecting these computer-managed assets (CMA)—assets that are managed through computer applications or can be manipulated or stolen with the aid and use of a computer—is vital to the financial and operational health of any organization.

A 2001 study by the Computer Security Institute and the FBI indicates that up to 85 percent of businesses suffer computer breaches each year. A separate study conducted by Exodus Communications shows that the dollar volume in losses caused by security breaches in the United States alone is over \$200 billion.

Due to the high value of their CMA, financial institutions are now increasingly required by both customers and regulators to implement specific internal security policies that dictate how information is managed and handled. Financial institutions must account for all user behavior and activities pertaining to those assets at all times, and document the activity in an audit trail. Healthcare institutions and other organizations are also under press to comply with similar, federally mandated auditing guidelines for regulations such as the GLB and HIPAA.

## **Trends in Security Spending**

The sheer size of an organization’s investment in their assets makes security strategy as vital as the assets themselves. But most businesses have concentrated their security efforts at the network perimeter, by way of authentication policies and firewall solutions designed to detect and reject unauthorized users and viruses.

While perimeter defenses remain an important element of security planning, their limitations are now clear to organizations in all industries that need to police not just the borders, but also the people, pipelines and repositories that constitute the enterprise system itself. Securing all of these elements is critical to ensuring business continuity. Which is why sectors like the financial services industry, for instance, will focus a great deal of initial 2002 IT spending on “disaster recovery, security solutions, and remote access systems,” according to an analyst at Framingham, Mass.-based IDC.

The trend is a microcosm of a broader strategic evolution away from hermetically sealing the network edge to acknowledging the statistical reality that hostile activity does penetrate corporate networks and often originates within the firewalls. Organizations are therefore implementing integrated policies throughout the infrastructure—borders included—that will make it easier to detect and mitigate threats at any point in the network and ensure CMA integrity.

### **Assessing the Cost of Infrastructure Attacks**

It is not an analysis that many company executives relish undertaking, but determining the financial impact of computer security breaches is the only way to make rational business decisions about protecting CMA elements. It is unpleasant, and is not easy, but the results of this analysis will invariably offer surprising insights to executives who are charged with managing the threats.

A leading analyst firm, Stamford, Conn.-based Gartner, has developed a structure for establishing a baseline estimate of the losses suffered by an IT infrastructure attack. According to Gartner, an accurate estimate requires examination of:

- the impact on the technological enterprise itself;
- the impact on staff required to respond to the incident;
- the impact of lost profit; and
- the impact on new clients who are unable to access the infrastructure.

Using these elements as the basis for a security breach impact analysis, Gartner developed a hypothetical model to explore the economic losses that would be incurred by a \$1.2 billion enterprise, with an IT support structure that enables 65% of realized profits, that was impacted by an incident that affects 35 percent of all system resources for a total of 72 hours.

Based on these parameters, the approximate losses estimated fell just short of \$1.4 million. Over the course of the incident, these hypothetical seed values resulted in a daily loss estimate of just under \$500,000, or about \$20,000 an hour over 72 hours. These numbers represent only the dollars lost to the IT infrastructure downtime. They go up dramatically beyond this when taking into account other losses that may also occur, such as fraud, file tampering, and theft of real or intellectual property.

Unable to prevent internal attacks altogether, some organizations have simply accepted some data theft or damage as normal shrinkage, just like retailers accept as inevitable some loss of inventory to employee theft. But as the above model illustrates, the losses incurred can be substantial. Fortunately, it is a fate that leading companies do not have to live with.

## **Tackling The Threat Within**

While heightened concern over cyber-terrorism currently dominates many organizations' information security planning, the most direct and statistically probable threats to CMAs actually reside within the enterprise, explains Umesh Verma, CEO of Blue Lance, Inc. (Houston, Texas), which provides real-time monitoring and auditing software to global businesses. He attributes the high incidence of "insider" security incidents to the accelerating pace of employee turnover, especially in recent waves of corporate lay-offs.

"More turnovers mean that more people know what's on your network and how to gain access," he explains. "But the most serious problem is that employees in a lay-off climate are prone to feel bitter, and to some degree, they may even consider that some corporate assets actually belong to them. It's not very surprising that companies have encountered more problems with internal data theft and even deliberate destruction over the last couple of years."

Altman agrees with Verma about the insider threat.

"With virtually all employees requiring some form of access to rapidly expanding corporate networks, the potential for abuse or accidental security breaches has increased significantly," Altman says.

In addition to the employee threat, there is that of business associates traditionally considered "outsiders" but who now have access to companies' IT infrastructure via e-commerce and extranet applications. The enterprise has now been extended outside of its traditional borders to include customers, partners, vendors and contractors. According to one analyst, this trend has increased the "insider threat" from the traditional 80-percent figure to an estimated 90-percent of all computer-related losses.

A 2001 Industry Survey conducted by *Information Security Magazine* also concludes that the majority of dollar losses from corporate security incidents are in fact from those perpetrated by "insider" sources. Curiously, that survey also found that 2001 corporate spending on information security remained focused on defenses against external threats, which suggests that most organizations are still unprepared to address their most serious security challenge.

## **Securing the Enterprise from the Inside Out**

An initial audit of most corporate security strategies will most likely find an imbalance that favors perimeter security over enterprise-wide monitoring. This gap clearly leaves company assets vulnerable to threats from within, the most common source of trouble for executives tasked with protecting their key business resources.

For the best protection, companies need to implement an "inside-out" security strategy that protects the organizational assets within the organization first, and then spreads out to the perimeter and beyond. This type of strategy prevents the all-too-common scenario of everyone being focused on external threats, while an insider is walking out the door with the company's crown jewels.

Workplace surveillance has raised concerns with some corporations over whether they would be considered by employees as “Big Brother.” However, in recent months, most employers are finding not only acceptance for internal monitoring, but actually a demand for it because of raised security concerns. This shift in attitude is enabling companies to implement inside-out solutions, and to talk about them with employees. The added communication has a side-effect benefit: experts agree that when employees know that strong monitoring technology has been implemented, the internal threat to CMAs is drastically reduced by deterrence.

### **Pairing Policy with Technology**

The ad-hoc approach to security infrastructure commonly found in large corporations is likely to leave gaps in enterprise system defenses.

“Rather than responding to each year’s security trend, companies should start from a carefully considered written security policy that states exactly what they need to achieve in order to protect their specific assets,” says Wayman Thurman, Director of North American Sales at Blue Lance.

In drafting a security policy to cover internal threats, administrators will need to identify which users have specific rights to which applications, data and enterprise resources. Once defined, this enterprise-wide policy should be applied to how CMAs are monitored and protected.

“Proper enforcement of rights and permissions needs to be reviewed routinely as part of any security audit. Day-to-day, the need to prove the policies are being adhered to should be addressed by implementing effective and discrete monitoring, reporting and alerting functions,” Verma says.

In order to effectively implement an inside-out security solution, administrators need to stop relying by default upon an existing palette of solutions that come part and parcel with application software that was not conceived with auditing, monitoring and alerting as their primary focus.

“Typically, large companies are not very well organized for security, having accumulated disparate systems that they’ve purchased without developing a coherent security policy,” reports Satish Kinra, Vice President of Sales at Blue Lance. “Over the years, they’ve simply used the tools that come bundled with Windows NT or Netware server software, which may or may not include monitoring, assessment, intrusion detection, forensics or other key capabilities.”

Tools are now available which can be customized to respond in a variety of ways to unauthorized actions. For instance, the monitoring system can be configured to stand by and record an audit trail of all user activity, so that intrusions can be traced back with legal certainty to specific users performing specific actions at specific times from specific workstations. At the other end of the spectrum, the system can trigger alarms to notify administrators that unauthorized actions are being attempted. More importantly, these policies can coexist.

## ***Protecting Computer-Managed Assets:***

---

Many CMA-rich organizations have even begun taking a “honey-pot” approach to security breaches, whereby monitoring systems allow detected attackers to proceed while recording attempted actions as evidence for prosecution while shielding assets from harm. Some critics may label such tactics as extreme, but when organizations are accountable to senior management and ultimately to shareholders for the security of corporate CMAs, the importance of deterring or preventing data theft, destruction and other crimes is vital.

In some sectors, maintaining audit trails of enterprise system activity is even becoming a regulatory necessity. Accountable to examiners from the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) for their security practices, banks are required to know at all times who is accessing and/or processing certain financial data. As they were before the computer age, the security practices of banks are critical not only for regulatory compliance, but also for customer confidence. As a result, banks are among the leaders in implementing network monitoring strategies.

## **Implementation Analysis**

With a comprehensive security policy document in hand, organizations are ready to implement a monitoring strategy over defined network assets.

The most basic by-product of a comprehensive monitoring strategy is a monumental volume of usage data detailing every aspect of network activity, ranging from users' identities to the files they access and what they do with them. Even in a small company, this volume of data would clearly overwhelm any effort to manually analyze it. That's why the all-important element of any centralized monitoring and auditing strategy is its data-management system, which relies on intelligent processes and automated tools to simplify collection, reporting, analysis, and continuous refinement of policies. Aided by software tools, implementing an effective surveillance and auditing program can be broken down into the following steps, according to Blue Lance CTO Peter Thomas:

**1. Taking Inventory of Computer-Managed Assets** – Administrators need to classify all of the different types of CMAs that reside on their networks. These could include technical documents, product specifications, marketing/customer data, competitive analysis reports, correspondence, agreements, quotes, invoices, purchases, budgets, revenue/profit/accounting data, salary/payroll, personnel details, and many other types of proprietary information specific to the enterprise.

**2. Establishing a Central Data Repository (CDR) of Audit Logs** – Many companies still have critical information stored in stovepipe systems, perhaps even on workstation hard drives. And most audit logs reside on individual servers. Moving audit logs into a CDR dramatically simplifies the monitoring and auditing process because all access pipelines—including those that deliver new data from sources—are known and controlled. With a CDR, organizations can report with certitude that they know exactly what is done to their data, when, and by whom. Establishing a CDR also simplifies the backup process.

**3. Ensuring Data Integrity** – Monitoring and auditing activity at the CDR actually makes it possible to trace all modifications of protected data. This means that, in the event of data corruption or loss, administrators are actually able to backtrack along the audit trail and recreate the original condition of protected CMAs, ensuring demonstrable recovery and integrity.

**4. Data Mining and Reporting** – Administrators need customizable, automated analysis tools in order to turn audit-trail data into intelligence. Monitoring systems should therefore generate real-time reports that can give security managers the ability to immediately perform forensic analysis, should a breach occur. They also need to deliver periodic reports that are meaningful to both tactical and strategic decision makers, so that security policies can be effectively refined over time to reflect each organization's specific usage and risk patterns. Without powerful reporting, organizations will not be able to demonstrate accountability to customers, shareholders, regulators, etc.

**5. Troubleshooting and Alarms** – Administrators also need to be able to define how their monitoring systems respond to data, application and/or network incidents. The ability to set alarms for any type of activity or condition is essential to any organization's centralized monitoring strategy.

**About the Sponsor: Blue Lance, Inc**

As a pioneer in information security, Blue Lance has proven its leadership many times over since its inception in 1985. In partnership with Novell, it developed the first totally secure, server-based audit trail technology. In 1996, Blue Lance became the first to develop consolidated reporting from multiple servers. Today, Blue Lance is the technology leader on many fronts and is the auditing visionary of the information security industry.

Blue Lance's flagship product LT Auditor+ is a real-time monitoring and audit trail security software solution, designed to secure organizational assets accessible through Windows 2000/NT and Novell networks. It protects against unauthorized access, fraud and theft through around-the-clock surveillance of network and user activity, real-time alerts, forensic analysis, and audit trail reports. Highly acclaimed by NetWare Users International, LT Auditor+ is in use by the world's largest corporations, banks, government agencies, education and healthcare institutions.

Altman Technologies distribute and support the LT Auditor+ product for Blue Lance and can be contacted as follows:

Tel: 01937 541400  
Outside UK: +44 1937 541400  
Email: [info@altman.co.uk](mailto:info@altman.co.uk)  
Web: [www.altman.co.uk](http://www.altman.co.uk)