

# DATA-WAREHOUSING SECURITY

The CEO stared hard at his chief corporate attorney, the bitter reality of the man's words still sinking in. The HMO for which both of them worked was being sued by patients whose confidential, on-line medical records had been electronically altered, by either outside hackers or a disgruntled employee with a grudge. It was already costing a fortune to double-check each record. By then word had leaked out, and now the class-action suit, alleging "multiple violations of privacy and patient confidentiality", sought damages in excess of one hundred million dollars. The HMO's outside counsel thought that amount was probably excessive, but they were certain that an out-of-court settlement was unlikely for less than fifty million. Worse yet was the attorney's latest piece of bad news: there was a strong possibility that the operating and settlement losses would trigger a stockholder's lawsuit against the CEO, his top officers, and the board of directors. Shaking his head in bewilderment, the CEO wondered how this had all happened. Data warehousing had been such an obviously right move; both for improved efficiency and lowered operating costs; and his CIO had assured him that the system would have password and virus protections. But something had gone, very, very wrong.

**THINK** this scenario is farfetched? If so, then you probably have a lot in common with most corporate leaders. In the last three years, this community has moved quickly to exploit the explosive growth of the data warehousing market. A new generation of analytical tools has arrived—better, more cost-effective and far easier for hard-pressed executives to use. Open access to corporate information holding has rapidly become the order of the day, the payoffs coming better and faster strategic decisions, more cost effective procedures and reduced overhead. Security issues, even when addressed, have seldom been an important part of the new corporate equation.

But gains often have hidden costs, and there have been some disturbing lessons from the dark side of high-technology, or what the military now calls "Information Warfare." During a recent tour of duty in Bosnia, for example, one of the authors found that viruses—some of them surprisingly sophisticated—had infected as many as fifty percent of the personal computers used by the

peacekeepers. Last year, the General Accounting Office reported that at least 250,000 attacks were occurring annually against Defense Department computers, destroying data and software. And in a situation that some liken to a potential "Electronic Pearl Harbor", a number of these attacks had installed "back doors" into DOD computer systems to facilitate surreptitious entry.

For business leaders, some even more startling parallels were reported in November 1996 by WarRoom Research in an unprecedented survey of Fortune 1000 companies. Nearly half of the 205 respondents admitted successful attacks on their corporate information systems by outsiders, with estimated costs per incident ranging from fifty thousand to more than one million dollars. And more than half of these companies indicated they had actually caught insiders—their own employees-misusing corporate computer systems.

These findings form the government and corporate worlds raise a number of basic security questions for data warehousing. The nature of technology means that data

warehouses share at least three common characteristics:

- They are compiled from data residing at many different organizational levels.
- Although data warehouses may be physically centralized, they are all most always accessed by users at many different locations.
- They are linked electronically, primarily through networks of client/server architectures.

However, these characteristics, each so necessary for the efficiency of the system, also represent individual and collective security vulnerabilities. To compensate for those vulnerabilities, data warehouses must contain the following defenses:

- Baseline protection against viruses at all levels;
- Internal controls and auditing mechanisms to prevent unauthorized access; and
- External controls to prevent penetrations and attacks by outsiders.

But there are major difficulties for today's corporate leaders in

By Kenneth Allard and Ramon Barquin

achieving these standards. The reason: a data warehouse contains the most valuable information assets that an enterprise can possess. These are treasure troves of bits and bytes mined by the organization at great expense in the hope of finding the lodestones of strategic direction and competitive advantage. It is difficult to conceive of a more lucrative target for penetration by the competition or a disgruntled employee seeking revenge. If enterprise integration has required a wholly different mind-set, then defending these treasures requires a similar change in attitudes. Above all, it means looking at enterprise security not as a disconnected series of seemingly random problems with individual technical “solutions,” but rather as part of an integrated, multi-disciplined strategy to build and protect enterprise integration.

With that approach in mind, how should the CEO be prepared to lead this effort?

### 1. Set and Enforce Security Policies.

It takes the concerted commitment of corporate assets, intellectual and physical, to create a data warehouse. But, if it is important or even vital to create such a resource, it is equally important to defend it. The WarRoom Research survey strongly suggests that corporate security policies fall short of this challenge unless they affect what the workforce actually does every day. As James Lightburn, a leading network and information security specialist puts it, “To achieve business continuity in this new ‘net-centric’ environment, the CEO has to set the standards for baseline protection and preservation of the enterprise information assets—and then enforce them.” And the only thing more important than setting and enforcing those standards? Insuring that the work force is trained and motivated to use them.

### 2. Insist on Multi-Disciplined Security

It is an unhappy fact of life in the information age that those who potentially threaten the data enterprise are utterly unconstrained by existing definitions, agendas or delicately balanced patterns of corporate responsibility. It follows that any strategy relying on either a single security “solution” or a series of randomly uncoordinated approaches is likely to fail. Computer Technology is increasingly a “system of systems.” As a result, information protection and preservation must be similarly multi-disciplined. Firewalls, virus protection, encryption, physical and operational security, as well as systems administration all have their place. But the CEO must insist that each of these disciplines be part of an overall strategy rather than individual components of piecemeal “solutions.”

### 3. Set Terms of Reference, Not Technology.

There are few more insidious obstacles to leadership than technology for its own sake. The CEO should be prepared to set the terms of reference for seeking out those technologies that can help secure the data enterprise. Those technologies should help him do the following:

- Detect and neutralize viruses at all levels of the enterprise;
- Identify and authenticate all users of the system—inside and out;
- Achieve active network management and control through a graduated system of access privileges. Who reads and writes what data and from what machines?
- Provide audit trails for all users of the data warehouse. Who went where and why?

Today’s CEO understands the imperatives of technology measured against the bottom line of earnings, profits and losses. Data warehousing has become a powerful tool in those

endeavors; but, as always, there is a balance to be struck. In the information age, the integrity of information itself is fast becoming “the risk of all risks,” with data warehouses as the most lucrative of all “high-value targets.” No CEO can leave these assets unprotected, any more than he would place corporate trade secrets in a safety deposit box and then hand out the keys to passers-by on the street. Asked why he robbed banks, Willie Sutton famously replied, “Because that’s where the money is!” In the information age, data warehouses are where the information is—so cyber-thieves are certain to try to loot them. We believe that the CEO is ultimately responsible for achieving the delicate balance between security and efficiency that this new era requires. But we suggest as well that what cannot be achieved through good leadership must frequently be managed by exception.

**DM Review**

---

*Dr. Kenneth Allard (Colonel, US Army, Ret.) is a recognized authority on information warfare. The author of several books on technology and security issues, he is associated with the Center for Strategic & International Studies and Georgetown University. He can be reached via e-mail at Allardck@aol.com*

*Dr. Ramon Barquin is not only an authority on data warehousing, but is also recognized as one of the pioneers in this field. The author of numerous publications, he is Chairman of the Advisory Board of The Data Warehousing Institute and is CEO of Barquin and Associates. He can be reached via e-mail at Rbarquin@aol.com.*

*The authors express their thanks to Mark Gembicki of WarRoom Research; James Lightburn of Lightburn & Associates and Howard Whetzel of Avenue Technologies for their*

*assistance in the preparation of this article.*