KEVIN CURRY

Managing information **security**

Daniel F. Lohmeyer, Jim McCrory, and Sofya Pogreb

Protecting proprietary information is becoming ever more important. To do so, many companies are looking beyond technology—and their technology managers.

Attacks on corporate information systems by hackers, viruses, worms, and the occasional disgruntled employee are increasing dramatically—and costing companies a fortune. Last year, US businesses reported 53,000 system break-ins—a 150 percent increase over 2000 (Exhibit 1). Indeed, the true number of security breaches is likely to have been much higher because concerns about negative publicity mean that almost two-thirds of all incidents actually go unreported.[1]

Although information security has traditionally been the responsibility of IT departments, some companies have made it a business issue as well as a technological one. This year we studied security best practices at Fortune 500 companies, particularly 30 that had recently appointed a senior business executive to oversee information security. (According to an April 2001 estimate by Gartner, half of the Global 2000 are likely to create similar positions by 2004.) A handful of these Fortune 500 companies are now adding strategic, operational, and organizational safeguards to the technological measures they currently employ to protect corporate information.

But most companies continue to view information security as a technological problem calling for technological solutions—even though technology managers concede that today's networks cannot be made impenetrable and that new security technologies have a short life span as hackers quickly devise ways around them.

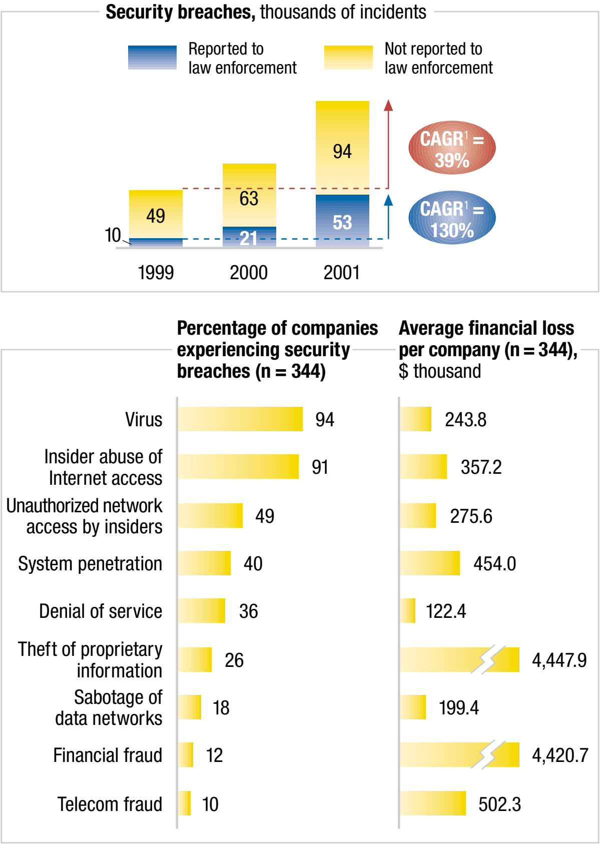
Delegating security to technologists also ignores fundamental questions that only business managers can answer. Not all of a company's varied information assets have equal value, for instance; some require more attention than others. One on-line retailer, Egghead.com, lost 25 percent of its stock market value in December 2000, when hackers struck its

[1] Computer Emergency Response Team Coordination Center, Carnegie Mellon University, Pittsburgh, 2002.

customer information systems and gained access to 3.7 million credit card numbers. Egghead, of course, had security systems in place and claimed that no data were actually stolen, but it lacked the kind of coordinated organizational response necessary to convince customers and shareholders that their sensitive data were actually secure.

EXHIBIT 1

Hackers, viruses, and worms



[1] Compound annual growth rate.

Source: *Computerworld*, January 2002; CSI/FBI Computer Crime and Security Survey, 2001

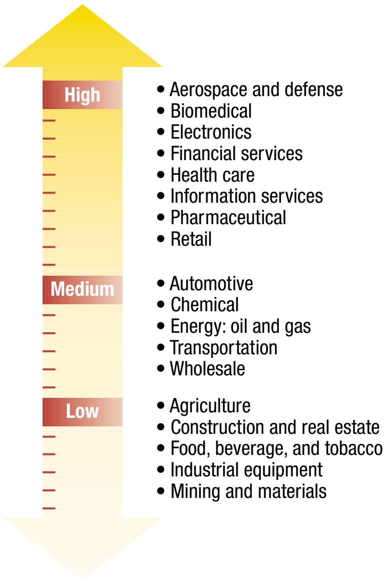
AOL Time Warner, Merrill Lynch, Microsoft, Travelers Property Casualty, and Visa International are among the organizations in our study that consider security more than just a technical responsibility: in each of them, a chief security officer (CSO) works with business leaders and IT managers to assess the business risks of losing key systems and to target security spending at business priorities. The CSO's decisions are informed by a deep understanding of the business and of the nature and degree of risk it is willing to accept.

Besides having a broader perspective on information security than IT managers do, CSOs at best-practice companies have the clout to make operational changes; the CSO at the personal-banking unit of a large European bank, for example, has the authority to halt the launch of a new product, branch, or system if it is thought to pose a security threat to the organization.

Only the CEO can overrule the CSO—and rarely does. In the typical company, by contrast, a security manager in the information technology unit

EXHIBIT 2

Variable degrees of risk



High:
- Aerospace and defense
- Biomedical
- Electronics
- Financial services
- Health care
- Information services
- Pharmaceutical
- Retail

Medium:
- Automotive
- Chemical
- Energy: oil and gas
- Transportation
- Wholesale

Low:
- Agriculture
- Construction and real estate
- Food, beverage, and tobacco
- Industrial equipment
- Mining and materials

has responsibility for security but little power to effect broader change in the system. In addition, CSOs at best-practice companies conduct rigorous security audits, ensure that employees have been properly trained in appropriate security measures, and define procedures for managing access to corporate information. When a decision is made to lay off or dismiss an employee, for instance, it is simultaneously entered into the human-resources system, thereby restricting that person's access to the company's premises, to e-mail, and to documents.

The role of information security, and of the chief security officer, varies by industry, the value of a company's data, and the intensity of the regulatory requirements it faces (Exhibit 2). At a health care organization, to give just one of many examples, the loss or alteration of records about patients could cause injury or death—an avoidable and therefore absolutely intolerable risk.

Today, most business leaders currently pay as little attention to the issue of information security as they once did to technology. But just as technology now stands higher on the chief executive officer's agenda and gets a lot of attention in annual corporate strategic-planning reviews, so too will information security increasingly demand the attention of the top team. In a networked world, when hackers steal proprietary information and damage data, the companies at risk can no longer afford to dismiss such people as merely pesky trespassers who can be kept at bay by technological means alone. Q

Dan Lohmeyer and **Sofya Pogreb** are consultants in McKinsey's Silicon Valley office, where **Jim McCrory** is an associate principal.