

FOCUS—Security

Securing the Enterprise

by Erik Sherman
Winter 2002

Senior management is abandoning its piecemeal approach to security and extending fundamental safeguards throughout the organization.

The tragic events of September 11 have caused smart organizations to revisit all aspects of security, both physical and IT. Companies are taking measures to reinforce what is, or should have been, common practice. Other avenues being pursued address basic assumptions—about people and about the world—that may no longer be valid. But what has become critical in the post-9/11 world is a change in attitude of management with regard to security.

Traditionally most industries looked at security as a pure cost. Even at many larger companies, managers saw little reason to invest in technology or people beyond a guard at the door and ID badges. This attitude started to change with the advent of e-commerce, when companies suddenly saw how vulnerable they were to outside forces as rogue technology experts corrupted or brought down corporate Web sites or broke in and stole sensitive information, such as customer credit card numbers. September 11 boldly underscored that vulnerability.

"[Security] is not on the back burner," says George Kurtz, coauthor of *Hacking Exposed* and CEO of security consultant Foundstone. "I spoke to one client today who said, 'Anything that has the word *security* in it is basically going to get pushed through.'"

Demand for security expertise has exploded since September 11. [Interfor](#), which counts government and corporate America as clients, has expanded "a few thousand percent," according to its president and CEO, Juval Aviv, "just to answer requests from companies about what they should have done years back and now are panicking about."

In some cases executives are focused not on a holistic approach to their organizations' security, however, but on a piecemeal approach, zeroing in almost exclusively on the kinds of vulnerabilities that were exposed on 9/11. "You have other areas [of security] crying out for help," Aviv says. "But because there have been no terrorist acts there, [companies] don't want to spend any money." In other words companies looking only at exotic scenarios could continue to ignore fundamental solutions: a well-lit parking lot to discourage crime, and locks and identification systems to restrict entrance to facilities.

For most organizations, though, the events of September 11 are forcing senior management to address these fundamental security measures.

Covering the Basics

The same basic principles and best practices apply today just as they did five months or two years ago. Business needs and requirements are the core of a sound security methodology; formulating policies and procedures, which are derived from an organization's business requirements, is the first step in defining an organization's security plan. "Effective security is a multifaceted process, with no single point of failure," says Kristin Parker, co-director of the Information Security Program at AMS's Center for Advanced Technologies. What should the most basic security plan address? Anything that could disrupt operations or reduce productivity. Proper preparation ensures that a business will continue.

"As people think about [security], they evolve into a preparedness mindset," says Gerry Samchuck, vice president of information systems and technology for Thomas Rutherford, an insurance brokerage company based in Roanoke, Va. "They're starting to focus on continuity of business." Although Samchuck has worked in corporate cultures that emphasize continuity, "a lot of businesses didn't think in those terms. It comes down to the simple things, from making sure your coworker is cross-trained to making sure your business processes are resilient: that you don't have single point of failure and that the infrastructure is resilient."

What's changed

Demand for security expertise has exploded since 9/11.

Current and future terrorist threats are forcing senior management to quickly address and assign fundamental security measures.

Executives must adopt new attitudes when considering security in a post-9/11 world.

Some executives are taking a more holistic approach to their organizations' security, looking at all aspects of physical and IT security that could disrupt operations and reduce productivity.

Some companies are focusing too much on vulnerabilities that were exposed around 9/11—such as anthrax protection—while overlooking or ignoring basic security measures.

Fundamental measures—policies that address whom employees may discuss sensitive information with and how to dispose of sensitive materials—should have been common practice pre-9/11. Since September 11, the fundamentals still hold true; the basics, including policies, locks, IDs, firewalls, and anti-virus software, must be covered.

Although it might be tempting to use September 11 as a reason to just hand security planning over to a consultant, passing off all responsibility can be a bad move. Security is intimately linked to a company's operations. A superficial familiarity with a business can result in real problems being overlooked.

"In our case that hasn't been necessary, because we do have that expertise and intimate knowledge," says Jim Wicker, vice president of information services for Dallas-based Dynamex, referring to the company's CEO and vice presidents, who all have strong operational backgrounds. "That also allows us to be more fluid in implementing change. We can quickly and efficiently implement changes that allow us to meet those new requirements." When consultants come in, they must become a part of a corporate security initiative, in which outside expertise can combine with detailed employee knowledge of internal operations.

Bigger Picture

As the trend of automating business over the Internet has increased, even Fortune 100 companies are exposed to potential security threats from partners and customers. For instance, a company may set up a solid architecture that includes a virtual private network for sensitive financial transactions that traverse a global network; however, if one of the company's enterprise partners has lax security policies that provide the possibility for anyone to access servers on the global network, the company's sound security principles are ineffective.

"Anyone who has access to a core or necessary part of your business is a risk," says James Williams, director of security solutions at [Solutionary](#) of Omaha, Neb. "If they don't invest in security, that creates a problem for you." The smaller the company, the more likely it might be a point of weakness.

The solution for smaller businesses wanting to do business with enterprise firms is to use managed service providers. "You get a piece of a best-in-class organization that there's no way we'd be able to afford," reports Samchuck. "Now you can put together an array of managed service providers to get the back room of a Fortune 100 enterprise." Larger companies can encourage their smaller partners to use a managed service approach to obtain appropriate security.

Right Attitudes

Whether it's e-mail worm attacks that compromise your systems or threats to travel that prevent you from meeting with clients, security threats can affect an organization's ability to connect with customers and partners and disrupt its service and operations.

To begin to identify the ramifications of security in a post-September 11 world means that executives must adopt new attitudes when considering security.

Dynamex makes 40,000 on-demand deliveries a day in North America and manages mailroom facilities for many buildings. When the planes hit the World Trade Center, customers, especially those in Manhattan, voiced concerns about safety. Management reaction was swift. "Our CEO immediately issued specific enhancements in security as well as restatements of existing security policies and procedures," says Wicker.

An important way to confront potential consequences is through role-playing exercises. "Before September 11, generally you'd find when you ran managers through a scenario that seemed at all unlikely, they would participate, but it would usually be accompanied by a statement that it could never happen," says Phillip S. Cogan, executive vice president at Bernstein Communications and a former communications official with the Federal Emergency Management Agency. Now, in 2002, nothing seems unlikely. With role-playing exercises, management teams can help shake previous attitudes and direct their organization through serious preparation.

A vital step is to move beyond expecting only those problems that have occurred before, says Ralph H. Kilmann, Ph.D., a professor at the University of Pittsburgh and president of Organizational Design Consultants in Newport Coast, Calif. He suggests organizing a corporate task force of 25 to 50 people from all areas, levels, and locations of the company. The task force tries to see the company as a

Who goes there?

One of the key problems in security is authentication, the process of ensuring that people are who they claim to be. Biometrics can identify people by unique physical characteristics, such as fingerprints, facial characteristics, or retinal patterns. Such devices can be useful, but only when users know their limitations.

Since September 11 biometric authentication has become the buzzword for security planning. But biometric devices are not the silver bullet. According to Robert Thompkins-Bey of AMS's Center for Advanced Technologies, facial recognition technology is notoriously inaccurate. One U.S. government study, for example, showed a 43 percent error rate of false negatives. "Biometrics are still a little flaky," says Richard B. Isaacs, senior vice president at [The LUBRINCO Group](#), "and they're better to identify a small number of people with a small number of errors than a huge number of people." In other words, they are best at authenticating a known group of people. That may be fine for employee identification, but it does little for a company concerned that terrorists, competitors, or irate outsiders might appear at the door.

Biometric systems are also only as good as the procedures that surround them. Incorporating biometrics into an organization's security plan is not the cure all—unless used in conjunction with other applications and part of an overall security policy for the organization. "Your security is only as good as your security check on the individual," says Andrew Szego, president and COO of fingerprint

hostile force—how a psychopath, disgruntled employee, enraged customer, or vicious competitor—might see it. "You bring in outside experts. You have to teach people about pathology, about psychotic behavior, about rage and anger."

An approach advocated by Bob Hughes, president and CEO of information security vendor [GuardedNet](#), is to create the corporate equivalent of a homeland security department. This group, reporting to the CEO or COO, would collect, sift, and analyze all information on security-related events and threats and then coordinate responses.

No matter what grand plans may result, however, without a change in attitude of management nothing will happen, according to experts like Kilmann and Chris Rush, CEO of security consulting firm Chris Rush & Associates. "They need to take off those rose-colored glasses," says Rush, who sees some change but is not yet ready to declare victory. "Many of us had this attitude that it will never happen to us. I for one never understood it, because of the attack in '93 on the World Trade Center and then the Oklahoma City bombing."

Of course, the real test of that change in attitude will come at budget time. That's when management must decide whether to pay the price for securing the enterprise. That can be expensive, but in the end it can prove a lot cheaper than the alternative.

Learn More



Consistent with heightened demands for in-depth security knowledge, the AMS Center for Advanced Technologies Information Security Program maintains a thorough understanding of security-related issues, technologies, methodologies, and trends.

The following resources are available from [AMS](#):

[AMS Technology Spotlight: Building Blocks for Securing Your Enterprise](#)

Security is an integral part of every e-commerce project, and security considerations must be included from the early planning stages, through implementation and after completion to validate the security of the system. A set of six core interrelated "security building blocks" are needed for secure e-commerce transactions from end to end.

[AMS System Security Engineering Methodology](#)

AMS's System Security Engineering Methodology provides end-to-end information security solutions that reflect and support business needs.

[AMS Security Assessment](#)

Through an AMS security assessment, organizations gain a fundamental understanding of their current state of security and receive an assessment of their current and future needs, an accurate risk assessment, and a realistic map to help them achieve business objectives.

AMS Threat Matrix

Understanding your risk is the first step in determining how and where to protect your organizational assets and the privacy of your information. The three major areas of risk-business interruption, information espionage and warfare, and information integrity-should be addressed with appropriate policies and procedures. Visit the [AMS Center for Advanced Technologies](#) Web site to view some examples of attacks and possible mitigation strategies for each of these three major types of risk.

Erik Sherman is a freelance writer and photographer whose work regularly appears in such publications as Newsweek and Technology Review. He regularly covers "Here and Now," an NPR syndicated radio newsmagazine. His latest book is Pocket PCs! I Didn't Know You Could Do That...(Sybex).

recognition vendor [SecuGen Canada](#). A clever thief, for example, might obtain a job under a false name with a target company. A biometric device will not keep such a person out. "Once you've established that your security checking procedures are adequate, biometrics can keep it secure," he adds. "But we're the second step, we're not the first step."

Although interest in the technology has grown, managers are still pulling out their calculators as part of their analysis. "We have to justify [biometrics] on an ROI basis," says Szego. "While we're into a more serious assessment of security risks and issues, financially, times are getting tougher. If we can reduce the cost of maintaining a password in an IT infrastructure, then we'll be considered as a viable alternative."