CSO
The Resource for Security Executives

June 2004 *CSO* Magazine

BUILDING THE FUTURE CSO

Feather Your Nest

While certifications are great, they won't get you into the boardroom. But one-stop shopping for a security education isn't there yet. It's up to CSOs to help change all that.

BY KATHLEEN CARR

COLLEGE IS GOOD. You get everything you need in one place. Classes. Peer networking. A meal plan. And a degree that proves you're qualified. But for the security executive, college is not good—well, not good enough, anyway. Yet. Because right now, there's no one degree that will land you a C-level security job. In fact, CSO might be the last executive-level position that requires you to cobble together your own education. "For new folks, the training ground doesn't yet exist," says Howard Schmidt, CISO of eBay. "There is no CSO institute. And colleges offer only an à la carte menu."

Today there's no one place for you to get your CSO credentials. "The job description and skill set requirements are still in draft form," Schmidt says.

On-the-Job Training
Information security leaders have relatively few options for pursuing a CISO-oriented degree, and it's even harder to find advanced academic degrees that focus on the corporate and physical side of security.

And that job description keeps expanding. A full-blown CSO position now includes such diverse security staples as video surveillance and network intrusion detection; but it also encompasses risk measurement and analysis, regulatory compliance, outsourcing, workplace violence and homeland security.

To put your current career on hold while embarking on any postgraduate program is daunting enough—and where would you find such a broad-ranging curriculum? Academia seems poised to develop programs, but so far, the pace is slow. You need to go to one place for your security expertise and another for risk management training—not an easy thing for the professional to do.

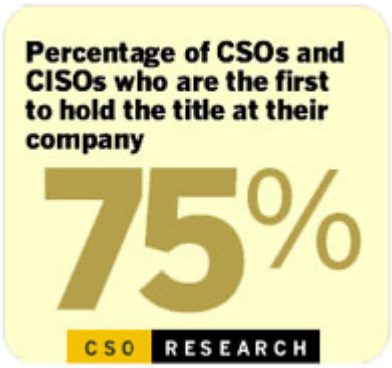
The information security community may be a bit further along when it comes to advanced academic degrees appropriate to executive-level security leadership. In fact, several programs offering an MBA in information assurance are under development. (For more on academic pedigrees in corporate and physical security, see "On-the-Job Training.") Many CISOs emphasize that the ideal CSO skill set includes a strong technology background coupled with a strong business sense. CSOs need to combine an understanding of risk management and governance with an awareness of legal and regulatory issues, and they need to know their audience, says Steve Katz, president of Security Risk Solutions. "It's a C-level job. And if we lose sight of that, we lose sight of the position we are filling."

Getting There From Here

It was 1999, and John Petrie was the technical services manager at Sprint. Petrie began his career with a bachelor's degree in international studies and military intelligence, but came to a crossroads the day his boss doubted his aspirations. The boss told Petrie he'd never rise to the

executive level because security personnel didn't understand the business. Today, however, Petrie is the CISO of the University of Texas Health Science Center at San Antonio. He had plenty of technical skills, certifications and experience. "But I didn't have the business theory; the know-how to do budgeting and accounting," he says. So he got an MBA.

He enrolled in an Internet-based MBA program at Washington State's City University, finishing his degree in March of this year. "I got an MBA because I had identified shortcomings in myself," says Petrie. "With it came the ability to determine the ROI of a project and to brief other executives on the risks of such a project."



Smart CSOs know that for security to work, it has to act as a business enabler. "But security people tend to be risk averse," says Mary Ann Davidson, Oracle's CSO. "Things are either secure or they are insecure." Businesspeople, on the other hand, are risk seekers, she says. "They know that if they don't take risks, they're out of business."

David Cullinane, CISO of Washington Mutual, agrees. "To function at the C level, you need to operate more as a business manager; you need to understand business requirements and processes," he says, "and you need to be able to discuss early adopter risk curves with the business managers. You don't need to discuss firewall settings with them."

For now, developing those skills means blazing your own path. Petrie was ambitious. He got his MBA while already serving as a CISO. And following recommendations set forth by the American Management Association and the Association of Professionals in Business Management, he also attended day seminars and took business courses on the side to improve his management skills—an approach that might be more feasible for those who can't quit their day jobs to go back to school.

The more education the better, says Will Pelgrin, director of the New York State Office of Cyber Security & Critical Infrastructure Coordination. He stresses that if you only have the technology background you'll need to develop your management skills as well. "You'll need to grow into a managerial role," he adds.

You'll also need to then translate the security needs to various audience members, including the CEO, the CFO and the marketing directors. "Whether it's through an MBA or simply a significant number of gray hairs in your head, you must [learn to] translate the technology to others," says Katz.

Stanley Jarocki, senior vice president and ISO of The Bessemer Group, goes a step further. "When I was young, I was a geek. As I matured, I had to sell the ideas I created. So I became a marketer," he says. His suggestion: Don't just present your ideas, become financially attached to them. "Then you're part of the budgeting process," he says. "I now have to put all of those pieces together and manage them. Today's security is just as much presentation as it is implementing. If we don't have awareness and buy-in, there's always someone who can undo what we put in place."

Jarocki notes that although risk management models differ across every industry, he's confident that the basic models of risk management can be taught. "If we give students those models, they will join the business world ready to tackle the risks," he says. "It'd be nice to do that at the college level, but we're not there yet," he says.

At some point in your career, you have to move from simply doing tasks to thinking more broadly about them. "If nothing else, you have to be able to articulate the risk issues in the

language of business," says Bill Boni, vice president and CISO of Motorola. "And the language of business is not limited to technology."

Boni is one of the founding members of a new group of security execs calling themselves The Global Council of CSOs. In addition to Schmidt, Davidson, Cullinane, Pelgrin and Katz, the group includes Rhonda MacLean, director of corporate information security at Bank of America; Scott Charney, Microsoft's chief security strategist; Whitfield Diffie, CSO of Sun Microsystems; and Vint Cerf, a senior vice president at MCI. The group's mission, according to Pelgrin, is to provide guidance both to academia and to the security profession to shape the CSO role.

At the group's first meeting, in November 2003, members worked on determining the ideal CSO skill set. The challenge, Boni says, was to define a framework for certification and training. "We didn't want to send people through a superficial orientation," he says.

It's an idea that The National Security Agency started six years ago when it began dubbing what is now a list of 50 schools as "Centers of Academic Excellence in Information Assurance Education." (For a list of schools see *www.csoonline.com/printlinks*.) Colleges and universities apply for the honor of being included on the list, and the students who attend the designated schools are eligible for federal scholarships.

"The NSA's list is a logical starting place," says Schmidt. "But it's tough for people to stop working and start a two-year degree." As an alternative, Schmidt has been working with Carnegie Mellon to develop a CSO institute for working infosecurity leaders, and to then share that information with other universities so that they can build their own programs as well (see "Campus Security").

Campus Security
Carnegie Mellon already has two master's-level programs that are good starting points for continuing education for CISO wannabes.

Read More

In addition, Eugene Spafford, a professor and director of the Center for Education and Research in Information Assurance and Security (Cerias) at Purdue University, explored the possibility of starting a CSO institute four years ago—but the external interest wasn't there at that point. Spafford hasn't given up hope; this fall Purdue will inaugurate an executive MBA program in information security that will allow CSOs to work independently on their degrees while spending a minimal amount of time on campus. He says the university will conduct market research for the CSO institute this summer that will include analysis of the enrollment in the executive MBA program.

It took decades for current CSOs to be viewed as valued members of the executive team. Those who are there now have put in their time. They have experience, and they've developed business skills either by finding a way to attend classes in their free time or by learning the hard way how to define security as something other than a cost center. Academia is on the heels of the profession's development. Just as many CSOs built their organizations' current security department, they'll need to do the same within colleges and universities to enhance the role and ensure that tomorrow's graduates have the education to do a CSO's job. If they don't, they'll have only themselves to blame.