InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

IT Careers: New Master's Degree Emphasizes Ethical Hacking

Don't expect to see a big crowd for EC-Council University home football games: The program's inaugural Master of Security Science class consists of only six students and all are taking their courses online.

By Larry Greenemeier, InformationWeek
July 19, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=201002295

It may only be July, but school's in session for IT security pros looking to develop the white-hat hacking, computer forensics, and other skills needed to help businesses turn the tide of today's security woes in their favor.

These abilities are essential to ensuring the next generation of chief security officers have what it takes to defend their organizations against increasingly more organized cyberattacks, and they form the foundation of the new Master of Security Science program launched this week by EC-Council, an industry group that offers training and certification to e-commerce and security pros.

While several universities offer master's programs that address information security, they generally follow curricula that are broader and more theory-based than the one created by EC-Council University, which takes its candidates through cyberlaw, disaster recovery, e-business security, IT security project management, Linux security, network security, secure programming, and securing wireless networks. The four core classes that must be completed for graduation address ethical hacking and countermeasures, investigating network intrusions and computer forensics, managing secure networking systems, and security analysis and vulnerability assessment. Students also must develop and present a research project.

EC-Council has been working since last August to form its own university based in Albuquerque, N.M., and license the university under that state's Higher Education Department. Don't expect to see a big crowd on campus for EC-Council University home football games: The program's inaugural Master of Security Science class consists of only six students and all of them are taking their courses via an online portal. Four of the students are from the U.S., one is from Latin America, and one is from India. All of them have an undergraduate degree in computer science or IT security. Some of them have master's degrees, but not in information security.

The total cost to complete the master's program is projected to be $21,400, which includes a $2,000

enrollment fee and a $2,300 graduation fee. The program is expected to take between one and two years to complete, depending upon the pace that each student can sustain.

The goal of the program, which is taught by a faculty consisting of nine professors, is to transform today's security pros into tomorrow's chief security officers and high-level security executives, although the school can't promise any particular job placement. Students are expected to study at the university half time, while working in the security field in some capacity. Attending school full time is counter to the spirit of the program. "It would make no sense if you didn't have any practical experience when you graduated," EC-Council president Jay Bavisi told *InformationWeek*. "A CSO position can't be attained only through academic studies."

There's plenty of room for more educational programs that properly prepare security pros for the challenges they'll face from day one in IT security environments, Stephen Northcutt, president of SANS Technology Institute, an educational organization licensed by the Maryland Higher Education Commission to grant graduate degrees in information security, told *InformationWeek*. Between SANS and EC-Council, "if we are both wildly successful, we will fulfill perhaps 1% of the market's true need," he added.

For that reason, SANS doesn't see EC-Council University as competition. Northcutt is, however, skeptical of college and university programs that offer only a concentration in security as part of their master's degrees in MIS or computer science. Such programs "are not qualified or equipped to properly prepare the students and end up wasting the student's time and financial resources and do not impart the technical and leadership skills needed to be effective in an era when the threat is at an all-time high," he said.

There are many academic programs that offer advanced IT degrees that treat security as a secondary component. Boston University, for example, offers an Online Master of Science in Computer Information Systems with a concentration in information security. Required courses for this program include network and software security, network management and computer security, and cryptography. Another school, Lawrence Technological University, offers a Master of Science in Computer Science with a concentration in computer security. Required classes at Lawrence include cryptography, distributed database systems and security, and security audit. Neither program's curricula mention white-hat (or "ethical") hacking, vulnerability assessment, or computer forensics.

The EC-Council in 2003 began offering certification for ethical hackers as a means of exposing defense-minded IT security pros to the ways in which malicious hackers operate. The next logical step for this form of security training was to introduce it as a formal academic program, Bavisi said. One of Bavisi's goals is to see more companies create CSO positions, even though he acknowledges that it's a fairly new title at most companies. "Over the past 15 years, CSO hasn't been a common title," he said. "You don't find that title at smaller companies."

Today's CSOs are in general well-educated in business, security, or compliance and auditing, and they play a high-level, strategic role within their organizations, Bavisi said. "But information security is a rapidly changing field, and the benefit of having a CSO with a Master of Security Science degree is that you will bridge the digital divide between security executives and their technical teams," he added.

Some companies may be concerned about investing in a CSO, adding an expensive employee to an area of the business -- security -- that's more of a cost center than a revenue generator. Others may be concerned that their employees will go through the EC-Council master's program only to leave for greener pastures when they've completed their degree. "People ask, 'What if I train my people and they leave?' " Bavisi said. "But, what if you don't train your people and they stay? Is paying for talent going to cost more than

succumbing to a cyberattack?"

Whether a company should have a CSO depends on its level of risk and the organizational structure. Bavisi pointed out that he's not suggesting that every company should have a CSO or that every security pro should have a master's degree. But with the state of computer security these days, it's clear that an influx of leadership in the security space could only help.