Cheaters - Inside the hidden world of IT certification fraud (Sep 08)

Industry launches counterattack using forensics, biometrics, analytics to weed out cert cheats

By Linda Musthaler , Network World , 09/01/2008

For the first time ever, companies that develop and administer IT certification exams are working together to combat a problem that has largely been swept under the rug for years: certification fraud.

A group of IT hardware and software vendors, independent certifying agencies, test centers and others have formed the IT Certification Council (ITCC). The goal is to share knowledge and resources to combat and prevent fraud, which is threatening to undermine the value of IT certification.

ITCC chairman Bill Horzempa, who is also director of Global Certification and Partner Education Development for HP, says, "Most of the members of this council have talked privately with one another about the cheating problem. We realized that this isn't just an HP problem, or a Cisco or Microsoft problem. Certification cheating affects the vendors, yes, but it also hurts individual IT professionals and the companies that employ or contract them. In effect, cheating creates a loss of confidence in the ability of the IT profession to solve business problems."

What is certification fraud?

"Certification fraud is any act, malicious or not, that is intended to help an exam candidate pass a certification exam using methods that violate vendor security policies." This includes acts perpetrated by certification candidates and corrupt test center proctors, as well as by the individuals and organizations that post and sell ill-gotten test materials on the Web.
Julieann Scalisi, Managing Director of Citrix Education

Chuck Cooper, ITCC vice chairman and program director, IBM Certification Programs Skills Enablement, Systems and Technology Group, calls certification fraud "an annoying pain that always seems to be there. It's a cloud hanging over us. It doesn't go away on its own."

Indeed, fraud in the IT certification industry is nothing new; the problem has been around for years. However, new techniques for analyzing test scores are making it easier to evaluate the scope of the problem. For example, test security company Caveon estimates that 15% to 25% of IT certification exams show some aberration, which can be an indication of cheating.

Ignoring the problem has only allowed it to get worse. All one has to do is Google the search term "MCSE study aids" and thousands of sites pop up where a student can purchase so-called test preparation materials – most of which are not authorized or recommended by Microsoft, the owner of the MCSE certification.

Though the documents are marketed as "study materials," the information often consists of stolen test questions and answers. Of course, Microsoft isn't the only company whose materials have been compromised. Content for virtually any IT certification exam can be found online.

The impact of certification fraud

Certification cheating has ramifications for everyone, including the individuals who pursue certification; the employers who hire them; the companies that contract for IT solutions and

services; the IT vendors who manufacture and sell IT products and solutions; the certifying companies and agencies; and more broadly, the general public.

What happens if you get caught cheating?

- Negation of test results
- Requirement to retake an exam
- Denial of a certification for a period of time
- Inability to register for exams for a period of time
- Loss of existing certifications or benefits from a vendor or agency
- Expulsion from a certification program
- Notification of loss of certification to the employer
- Civil or criminal prosecution
- Cease-and-desist order for the sale of stolen test materials

The individual who cheats is taking a risk with his career. If students are found to be cheating, they can face a range of consequences, such as negation of their test results; loss or denial of certifications; banishment from a certification program; or notification to his employer. Each certifying agency sets its own security policy which should be understood before a candidate undergoes the certification process.

Employers also suffer when individuals cheat on certification and are not truly qualified for a job. "If employers aren't getting quality work out of their employees, they are being defrauded," according to Taylor Ripley, chief security officer, CertGuard. "Employers need to know they are getting what they ask for."

Ripley says the companies that are most likely to suffer damage from certification fraud are the smaller size companies that don't have a Human Resources department to help weed out people who can't do a job. "These companies are forced to rely on certifications to judge a person's qualifications. A small company could lose money or business if an unqualified person screws up," Ripley says.

The VAR factor

But sometimes it is employers who encourage employees to get certified using any means necessary. For example, a systems integrator or value-added reseller (VAR) might want to get authorized to sell a particular vendor's product. Authorization might require that the company have one or more certified professionals on staff.

"If a VAR helps his employees cheat to get a certification in order to get or stay authorized, the company's customers are affected, as well as the vendor that the VAR represents," Ripley says. "Say someone cheats to reach the Microsoft Gold Certified Partner level. If the VAR implements a poorly designed solution, the customer has wasted his money and he thinks Microsoft has bad products. Everyone loses when this happens."

Rick Gregory, managing director of the training community of TrainingIndustry.com, has heard of instances in which outsourcing contracts are being canceled and the work is being brought back in-house because the people assigned to the contract simply weren't qualified. "The contract specified a requirement for specific kinds of certified professionals, so the people went out and

purchased a credential," Gregory says. In the end, the work was below standards set in the outsourcing agreement.

Vendors such as Microsoft and Cisco and third-party agencies like the Computing Technology Industry Association (CompTIA) and the Storage Industry Networking Association (SNIA) that sponsor certification programs lose both money and intellectual property when even one exam is compromised. It can cost hundreds of thousands of dollars and take numerous subject matter experts three to six months to develop a certification test.

"We hear from candidates that some of our tests are readily available," IBM's Cooper says. "It's a compromise of our [intellectual property]. Our internal sponsors wonder about the validity of the tests. They typically don't need to rewrite the tests, but they need forensics to understand the impact to the test scores. Nevertheless, the perception is that damage has been done."

Fraud and the countermeasures

In order to develop measures to combat fraud, the certifying agencies need to understand how cheaters operate. Here are some of the cheating techniques that have been identified and what authorities are doing to thwart the fraud.

One of the oldest tricks in the book is to get someone else to take the test in place of the real candidate. Called a proxy test taker, a person goes to a test center and takes an exam registered as someone else. A few "entrepreneurs" have even turned this technique into a business.

"Recently we found that our certifications, along with other IT certs, were being sold on the Internet via a proxy test taking service," says Julieann Scalisi of Citrix. "Caveon, as part of our new Web patrol service, took the action to have them removed from Google. Unfortunately, the site still exists and they appear to be selling Citrix certifications from $700 to $4,800."

Cisco and test delivery company Pearson VUE are in the forefront of implementing stringent candidate authentication techniques to discourage proxy test taking. Soon, each Cisco exam candidate will be required to have a digital photo taken at the test center, and must provide a digital signature in order to take the exam. The photo and signature will be attached to the test results.

Over time, Cisco and Pearson VUE will be able to spot individuals whose photos appear under different names and signatures. Other vendors and test delivery companies are exploring the use of biometrics such as fingerprints to determine if one person is taking tests under numerous names.

Erik Ullanderson, manager of Global Certifications for Learning at Cisco, is happy to share his antifraud techniques with his colleagues on the IT Certification Council. "Our efforts in curtailing fraud are not a Cisco-only value-add," Ullanderson says. "We think other companies should be jumping on the investments that Cisco and Pearson VUE have made." Indeed, the ITCC is looking at how it can utilize this and similar programs worldwide in light of privacy concerns in various countries.

Another common cheating technique is to have the test items and answers in advance. Such information is often posted to certification forums, blogs or brain dump sites, giving a candidate the opportunity to memorize rather than actually learn the subject matter. "We know that exam content can be found on different Web sites for a fee," Scalisi says. "Content and answers also can be found within blogs and discussion forums that are usually intended to help others answer difficult exam items, sometimes providing hints but often times providing actual answers."

More blatant are the Web sites that sell hundreds of actual exams, marketing them as study aids. "Certification candidates need to know that certifying agencies never provide their exams or other preparation materials to these brain dump sites," HP's Horzempa says. "Most of what is posted has been obtained through illegal means." In fact, brain dumps are often a violation of the laws protecting copyrighted intellectual property.

Targeting the consumer

This, then, begs the question: why don't authorities shut down the brain dump sites? Because it's not as easy as it seems.

"In the late 1990s, the Digital Millennium Copyright Act (DMCA) gave software companies and testing centers the ability to go after unauthorized providers of test content," says David Meissner, vice president of Solution Services at Prometric. "But having this legal tool doesn't make it easy to go after the offenders. Often they are located in countries that don't recognize U.S. laws, making prosecution difficult to impossible."

It takes very deep pockets to pursue the purveyors of brain dumps. Civil or legal action can drag out for years with little success to show for the effort. Many certifying agencies will pursue a cease-and-desist order rather than a lawsuit if their intellectual property is compromised.

A different strategy for combating certification cheating is to go after the consumer of the illicit materials. "Brain dump sites are like drug dealers," says Lee Futch, product management lead for Symantec Education Services. "As long as there is a customer, there will be a dealer. We need to cut off the customer base to kill the illegal dealers of stolen [intellectual property]."

One of the missions of the ITCC is to spread the word to candidates that the certifying agencies are indeed going after the consumers of the stolen test materials whether the consumption was intentional or inadvertent.

The good news is that it's getting easier to spot cheaters. Using new data forensics techniques that didn't exist just a year or two ago, certifying agencies now collect metrics that can indicate the possibility that someone has used illegal tactics to pass the exam.

The metrics reveal statistics such as how long it took the student to answer each test item, which answers were changed during the test, and how much time the student needed to complete the test. These metrics are compared with a historical baseline value, and too much variation raises a red flag. Before the student even walks out the door of the test center, the test results can be called into question, triggering further investigation.

Even "inadvertent cheaters" can be caught this way. People who use information from the brain dump sites are essentially able to memorize or at least practice actual test questions and answers, whether they do it knowingly or not. This advantage can be readily identified in the test metrics, and the candidate can be singled out for further investigation and possible consequences.

"Citrix uses data forensics to identify specific instances of cheating," Scalisi says. "We now conduct a monthly review to identify anomalous scores and results. Once confirmed as cheating, candidates are subject to remedies up to and including certification revocation and ban from testing for up to one year."

ITCC members don't share data forensics about specific exams or individuals, but they do share information about testing centers if corruption is suspected. "Forensics let us look across tests

and centers around the world," IBM's Cooper says. "When a test center appears to be compromised, we gather statistically valid proof to act upon. This data is based on tens of thousands of tests that are administered each year."

One test developer who prefers to remain anonymous describes a recent scenario in which dozens of candidates took the same exam at a proctored testing center in India. Every candidate scored extremely high on the test -- a definite aberration from normal circumstances. "This was an indication to us that the test center had a security problem," says the developer. By sharing such information through the ITCC, the IT vendors can decide whether to continue using that testing center.

It all starts with the test

Test developers are adding new measures of security into their exams. Prometric's Meissner says innovation in test security will help curtail cheating. "There are new ways to assemble a test to incorporate security," Meissner says. "For example, a fixed form test that has 100 items would be easy to memorize. By adding item cloning, in which there are three or four variations of the test, the full test is much harder to memorize. Making the test modular creates even more variations. Even better, dynamic forms use a computer system to generate a unique test for each candidate." All of these techniques make it harder for people to memorize and regurgitate the test for profit.

Futch says Symantec is taking a bit of a "fight fire with fire" approach to exams. "Symantec uses multiple versions of a test for each certification exam, and we use stealth questions embedded in the tests to determine if people have used brain dump sites to prepare," Futch says.

Several vendors, including Microsoft, HP, Citrix and Cisco, use performance-based testing, a method that includes a hands-on portion of the test that is difficult to fake. The test taker uses a simulator or a virtual environment to perform specific actions that help him derive the answers to test questions. In addition to being a better way to judge a person's knowledge of the subject matter, performance-based exams reduce the possibility of cheating. This type of exam is more difficult and expensive to develop, but new innovations in virtualization and animation are making it easier to develop and administer the exams.

Citrix is adding a "why" element to its exams. "We have a quality initiative within our courseware development team that is focused on including the 'why' in our course content," Scalisi says. "This will help ensure that our students not only learn how to perform required tasks but why it's important as well. Going forward, our exams will likely include this, making it more difficult or impossible to memorize answers." She points out that one of the exams associated with the Citrix Certified Integration Architect (CCIA) certification track tests candidates' ability to make design related decisions and then advise why they made their decision.

Certification is still a good measure of skills

Horzempa stresses that the certification process is still important to employers looking to hire qualified IT professionals. "The vast majority of people who have attained certifications have done so legitimately," Horzempa says. "They have studied hard and applied their experience and knowledge to prove they are experts in their field. Employers can still have confidence in using certifications as one measure in evaluating candidates for employment."

On rare occasions, people may claim to have credentials that they really don't have. "Employers can always contact a vendor directly to verify that a person holds a credential," Gregory of TrainingIndustry.com says. He compares it with verifying employment history when candidates

list previous employers on a resume or application. Most certifying agencies will verify whether a person has attained the credentials he lists on his resume.

As Scalisi points out, certification that is earned legitimately validates that a person possesses the qualifications that will help him perform a job successfully. Thus it is in everyone's best interest to maintain the integrity and value of the IT certification system.

"There will be people who cheat no matter what," Horzempa adds. "To them, the risk of getting caught is worth the reward of making easy money. But there are many more honest people that might be tempted to cheat – say, by buying a 'study aid' that is really a copy of the exam – that must now ask themselves if the penalty is worth the risk. Is it really worth ruining your career and destroying your personal integrity if you get caught cheating or selling the exams? To these people, I simply say, 'Study for the test, and take it legitimately.'"