

Employers Beware: Degrees And Certifications Don't Guarantee The Quality Of An Information Technology Applicant


Joseph M. Zadik, (Graduate Student), Purdue University, USA
Kevin Dittman, Purdue University, USA

ABSTRACT

Due to the shortage of qualified information technology (IT) professionals and the supply of available IT jobs, a new industry has surfaced in search of profits. Many individuals and organizations seek to either bypass the traditional educational process or obtain fraudulent credentials with the purpose of securing a high paying IT job. This paper discusses the trend of fraudulent credentials, their impact on organizations, and reasons why the quality of information technology job applicants cannot be guaranteed based on their degrees and/or certifications.

Keywords: Information Technology, Certifications, Diploma Mills, Brindumps

INTRODUCTION

 ver the past 40 years, mainstream computing has been integrated into the fabric of our society. More importantly, it has been injected into the important day-to-day operations of government and business. When applied correctly, information technology (IT) has the capability to improve and transform the way services are provided and the way information is handled. Leaders look to IT professionals to implement technology for competitive advantages or as a means to improve processes and reduce costs. They also look to the same IT professionals to define, lead, and successfully implement the projects. Unfortunately, as IT professionals we don't have a good history regarding IT project implementation. The 1994 CHAOS report states that "in the United States we spend more than \$250 billion dollars on IT application projects" (The Standish Group 1994). It is likely a large amount of those funds were wasted because of poor project management and low quality deliverables. Additionally, the report provides other staggering statistics about IT projects:

- 31.1% of IT projects will be cancelled before they ever get completed.
- 52.7% of IT projects will cost 189% of their original estimates.
- 16.2% of projects are completed on-time and on-budget on average.
- 9% of large corporate projects are on-time and on-budget.
- 42% of completed projects have the originally proposed features and functions.

Unfortunately, the project success rate has not improved much since 1994. A 2004 report by the Standish Group updated the demographics provided by the CHAOS report. The most important statistic is that only 29% of IT projects are successful. The report defined the term "successful" as on-time and on-budget with required features and functions (The Standish Group 2004).

Research has focused on discussing the impact of scope, cost, and management on IT projects. An important factor has been overlooked - the quality of the IT employees implementing the technology. Did the quality of the team contribute to the failure? Were failures caused by an employee's misrepresentation of his or her background and/or knowledge?

The purpose of this paper is to discuss fraudulent credentials, their impact on organizations, and reasons why the quality of information technology job applicants cannot be guaranteed based on their degrees and/or certifications. The scope of this paper is limited to universities and corporations located in the United States.

DEGREE AND CERTIFICATION QUALITY

Two varying factors that affect the effectiveness of IT departments are employees' degree quality and certification quality.

Degree Quality

From the general perspective of a student, it is likely the quality of a higher education degree is based on four factors: the institution's reputation, size, student/instructor ratio, and the employment placement figures of graduates. Although in some cases the quality of the degree or institution might not matter. Some people strive to attend the best schools while others are satisfied with simply receiving the sheepskin. In fact, some people are even willing to purchase a fake degree in a fraudulent misrepresentation of a higher education.

Degree quality is relative; it wholly depends on the assessment metrics and how they are evaluated; therefore, some degrees are perceived higher quality than others. According to U.S. News and World Report 2007 rankings (USNews.com 2006), the number one university in the United States is Princeton University. If a prospective employer has one applicant from Boston College (#34) and the other from Princeton University (#1), it is likely the latter will be viewed as a higher quality candidate because of the institution's perceived quality. One issue arises when comparing applicants from less known colleges, universities, or trade schools. For example, what about a candidate from Trinity Southern University versus a candidate from Trinity University? It may be surprising to know that the first institution is actually a "degree mill" that churns out fraudulent degrees, while the second is a well-regarded university in Texas ("degree mills" will be discussed in more detail later in this paper).

According to a University of Florida website, the quality of a degree is determined by a combination of four factors: faculty knowledge, course content, instructional strategies, and student commitment (UFL.com 2006). For an information technology degree, factors such as quality high-tech facilities, corporate partners, and job placement are also important. Additionally, the university's or program's accreditation is significant. The topic of accreditation will be discussed later in this paper.

Certification Quality

Around ten years ago, technology vendors started certification programs as a benchmark by which information technology professionals could be compared against to validate their stated skill level. These certification programs had varying levels of difficulty and usually provided monetary corporate rewards to those who passed. In our society, if there is a financial reward, then someone is probably trying to cheat the system to receive it. Certification programs are not immune; the potential for monetary gain and improved job placement lead to an invasion of groups trying to cheat the system.

Counterfeit vendor certifications can also be purchased online. An internet search returned a live auction for counterfeit certifications from vendors such as Microsoft. Fortunately, the awareness of counterfeit certifications and the ways to recognize them has improved. Many companies now require more information to validate a certification. Simply showing a certificate is no longer good enough. Therefore, this form of cheating will be the first to disappear.

The largest form of cheating related to certifications comes from a "braindump," also known as material provided to people that enables them to memorize stolen exam questions and answers in order to pass the exam. A "braindump" is compiled in a simple manner. People are paid to take a certification test and then write down the questions they remember promptly after the test. After the requested questions are delivered, the answers are compiled and the "braindump" is then sold to test-takers as a study guide. Having such a study guide leads to people who cram for a test by memorizing the questions and answers yet have little true expertise in the subject. Therefore,

while a person may have a valid certification as a Microsoft Certified Systems Engineer (MCSE) for example, he or she only memorized answers and has no applied knowledge. While working in industry, we have heard the term “paper MCSE” coined for such individuals. Unfortunately, the manager and corporation who hired these people usually do not find out about their real experience until a project fails or another catastrophe occurs because of the individual’s true lack of experience.

Robert Williams discusses “hired guns,” a new form of cheating, in his article “Braindumps, Gunman and Cheaters” (Williams 2006). “Hired guns” are an elite group of IT thieves who will actually take an exam for someone who has features similar enough that they could pass for each other based on picture identification. The majority of these “hired guns” are located in India and China where this practice has been huge among college students.

CREDENTIAL FRAUD AND DIPLOMA MILLS

As we read through several message boards and had discussions with colleagues, the phrase “guilty by association” came to mind. There were discussions regarding the quality of employees – a failed project, a lack of knowledge, a lack of fundamentals. Each time the complaints were followed by the person’s credentials for example, “The person claimed to be a CCIE” or “the person has an MCSE but was worthless.” These comments illustrate how credential fraud could affect a student in higher education. If a hiring manager has had a bad experience with a graduate from the same college or a holder of the same certification, how would his or her prior impressions affect the student’s opportunity for employment? Considering most applications only get a quick glance during review for a position, it is likely that ideals related to past experiences would carry over and create a negative effect on potential future employees. Does a person’s misrepresentation cause a degree or certification to have less value? Yes, it likely has an affect on the value.

Over the past fifteen years, the existence of organizations offering fraudulent credentials from fake schools, as well as counterfeit degrees representing real schools and vendor certifications, has greatly increased. For information technology, two large concerns are “diploma mills” (a.k.a. “degree mills”) and counterfeit vendor certifications. A “diploma mill” is defined by the US Department of Education as “an unaccredited institution or other educational providers that have been repeatedly denied recognition and/or persecuted as frauds by state governments” (ED.gov 2006). In further detail, the Oregon Office of Degree Authorization adds that:

diploma mills (or degree mills) are substandard or fraudulent “colleges” that offer potential students degrees with little or no serious work. Some are simple frauds such as a mailbox to which people send money in exchange for paper that purports to be a college degree. Others require some nominal work from the student but do not require college-level course work that is normally required for a degree (OSAC 2006).

According to an Associated Press article from December 2004, the Pennsylvania Attorney General’s office filed a lawsuit against the owners of the online university Trinity Southern University in Texas after the deputy attorney general’s cat was awarded an MBA and 3.5 GPA. In May 2004, TV news station WTHR in Indianapolis, Indiana conducted an investigation into “diploma mills” And found that more than seventy workers were facing layoffs from Chrysler Corporation. The employees decided to take advantage of the company’s tuition assistance stipend and enrolled in an online program at St. Regis University. Unlike traditional college students, these workers received degrees on the internet without ever taking a class, at a cost of \$42,000 to the Chrysler Corporation. The investigation uncovered that St. Regis University was a “diploma mill” (Chapman 2004). The story prompted a federal investigation involving the Secret Service, Homeland Security, Immigration, the IRS, and U.S. Postal Service. In October 2006, WTHR published a follow-up story regarding St. Regis University. During federal hearings it was revealed that numerous government employees had purchased fake degrees including a White House staff member, members of the National Security Agency, a Senior State Department Employee and a worker at the Department of Justice (Chapman 2006)

In fact, not even the law enforcement community is immune from credential fraud and fake degrees. In July 2006 two Naples Florida veteran police officers were fired after it was discovered that they received incentives for degrees which were obtained through an online “diploma mill” called Almeda University. The police officers were

terminated after many years of service and are repaying the department for incentives received because of the degrees. Following a three month fight, the officers were recently reinstated in the Naples Police Department (Mills 2006).

Unfortunately, “diploma mills” are not the single source of the problem. There are also websites that will create counterfeit degrees for well-known schools under the guise “novelty entertainment.” A search of the internet produced a couple of websites dedicated to the re-creation of such degrees. The website “truecounterfeitdiplomas.4-all.org” proudly displays how it can reproduce a degree for \$400.00. Additionally, the website “nd-center.com” provides a degree and the associated transcript for \$400.00.

PERSONAL ETHICS

Situations also occur where people deliberately lie on their resume regarding their qualifications and later are caught. In February 2006, David Edmonson, Radio Shack’s former president and CEO, resigned when questions arose about the qualifications stated on his resume. He claimed to have received two college degrees but an investigation proved he had never graduated from the college in question (USAToday 2006). According to MSNBC, during his approximately 10 month tenure the company’s profits plunged and Radio Shack announced plans to close up to 700 stores, hinting at his lack of qualifications (Associated Press 2006).

Beyond credential fraud, hiring managers in information technology should be concerned with compromising security, in addition to several other aspects of IT. Because of the nature of IT, many positions within the field have access to restricted corporate and personal information. A system administrator for example, can access all digital employee files including data such as email, compensation information, and secret corporate information. In April 2005, a report was released regarding a lady who was hired as a contractor for the Teachers Insurance and Annuity Fund – College Retirement Equities Fund (TIAA-CREF) to test databases. Just days before starting, she was sentenced to four years in prison for helping her friend steal \$200 million from insurance firms. This conviction was undetected and she worked at TIAA-CREF for nearly two months with access to customer data from a number of colleges including Harvard, the University of Michigan, and Purdue (Gasparino 2005). Additionally, since IT employees often purchase the hardware and software, corporations can also be victims of such theft. In June 2003, a Microsoft employee was indicted for ordering \$17 million worth of software through an internal purchasing program then selling it and keeping the profits (Reuters 2003). Hiring managers in IT departments should look at resumes and other documentation with scrutiny to avoid hiring fraudulent and lackluster employees who have access to sensitive information.

RECOMMENDATIONS

Because of the potential for personal financial gain, fraudulent activity will always be a part of our society. To improve the likelihood of hiring a quality employee versus a fraudulent IT employee, we recommend the following process: Investigate, Validate, Educate, and Report.

Investigate Institution Credentials

The investigation phase should be comprised of researching and examining the institution’s classifications and accreditations.

Research school classifications

The Carnegie Foundation for the Advancement of Teaching has a formal classification system for U.S. Higher Education called “The Carnegie Classification of Institutions of Higher Education” “<http://www.carnegiefoundation.org/classifications/>”. This report provides the user an opportunity to filter schools by specific criteria such as school size and degrees offered. This reference can be useful as an initial point of investigation if the authenticity of an institution is in question.

Examine the institution's accreditations

The goal of accreditation as defined by the U.S. Department of Education is “to ensure that education provided by institutions of higher education meets acceptable levels of quality” (USDOE-OPE 2006). The United States does not have a central authority to maintain a single point of control over all postsecondary educational institutions in the country. Each state has a varying degree of control over education. In general, higher education institutions are allowed to operate with a considerable amount of independence and flexibility.

While there are many functions of accreditation, two apply directly to the scope of this paper. First, verifying that an institution or program meets established standards provides a strong foundation for determining its credibility. The lengthy verification process is conducted by private educational institutions known as accrediting agencies and consists of specific evaluation criteria. Secondly, as a precaution for prospective students, it provides a framework to assist in identifying acceptable and respected institutions. To aid in these two functions:

the Secretary of Education is required by law to publish a list of nationally recognized accrediting agencies that the Secretary determines to be reliable authorities as to the quality of education or training provided by the institutions of higher education and the higher education programs they accredit (USDOE-OPE 2006).

The U.S. Department of Education recommends that the database it provides be used as a source of qualitative information and that additional sources should be referenced. Not only are such databases a valuable resource for prospective students, they should also be referenced by employers who question the academic institution from where an applicant indicates a degree was awarded.

As a complement to general accreditations that apply to an entire institution, there are also program-specific accreditations. The Association of Computing Machinery (ACM) recently approved an accreditation program to establish standards for undergraduate information technology degrees. The Special Interest Group for Information Technology Education (SIGITE) “<http://www.sigite.org/content/index.maml>” adds a level of validation to information technology programs by requiring that specific standards are met – in addition to the general standards for computing programs defined by the Accreditation Board for Engineering and Technology (ABET).

Validate The Information Provided To Identify Fraudulent Credentials

The validate phase should be comprised of validating the vendor’s certification, the applicant’s background, and requesting official transcripts from the applicant’s institution.

Vendor certification validation

Many vendors provide an area on their corporate website where their certifications can be validated. Usually the process is as simple as entering a certification ID number. In most cases, the data returned will include the person’s name and what certifications they received. If the certification ID is not valid, some sites simply return nothing while others will redirect the page to a website for reporting fraud specific to the vendor credential being validated. Either way, it is a simple step that reaps generous awards for the protected employer. For example, the Project Management Institute website to verify PMP certifications is: “<https://www.pmi.org/CertApp/Registry.aspx>”.

Applicant background validation

There are many businesses that provide background validations and investigations. Considering the level of organizational access employees in information technology may have, this should be a standard part of the hiring process. Background investigations provide varying levels of information about the applicant in question. For example, the investigation can provide results about anything from criminal convictions to all public information on record about the applicant (including his or her driving record and credit history). However, while a wealth of information about the subject can be provided and prove to be very useful for the hiring organization, such investigations can be very expensive.

Request official transcripts

The applicant should approve to have his or her official transcripts sent directly from the institution from where they graduated to the potential employer. While there is always the risk of transcripts appearing official but in actuality

being fraudulent, having the transcript sent directly from the accrediting institution to the potential employer can reduce the risk of fraud. In addition, the validation of an institution and its accreditation can provide additional legitimacy to the transcript.

Educate Information Technology Professionals About The Resources Available

One way to fight fraud is industry education. As more professionals in the IT industry become aware of credential fraud and apply techniques to validate information, the likelihood of hiring a poor quality candidate based on these factors should decrease. With the declining rate of hiring employees with fraudulent documentation, the risk associated with getting caught and reported will soon outweigh the potential rewards.

Report Applicants Or Employees Who Present False Credentials

Microsoft, for example, has an area devoted to stopping piracy related to its certifications "<http://www.microsoft.com/learning/mcp/program/piracy.asp>." The company provides a lot of information on the problem and ways the industry can fight back, including a hotline to directly report people or companies participating in "braindumps," "hired guns," or certification replication.

CONCLUSION

Historically, the success rate and quality of information technology projects has been poor. Industry certifications such as the PMP, MCSE, and CISSP were developed to provide a quality benchmark for employees to be compared against, but have been weakened by fraudulent documentation. In addition, the knowledge and experience gained through post-secondary education is a critical step to being an effective information technology employee.

Having such credentials can lead to employee financial gains (i.e., increased salaries); therefore, people who are unwilling or unable to learn the material will try to cheat the system. Organizations which provide services such as "braindumps," "hired guns," and fake degrees or certifications create the means for unethical people to attain credentials they otherwise wouldn't have.

However, it is inevitable that those who cheat will end up in a situation in which their lack of knowledge is displayed, but usually at the expense of the hiring organization's reputation, credibility, and bottom line. As previously discussed, there are two main reasons why this is negative for a corporation. First, the employee's inadequacy may lead to a project or product failure. While the impact of the mistake will vary, past instances have led to lost revenue and media scandals. Second, an unethical and fraudulent person shouldn't have the privilege of being entrusted with an IT position in which he or she has access to confidential information.

To maintain the credibility of degrees and certifications, companies with such requirements must do their part to fight fraud by guaranteeing that they are doing all they can to prevent hiring fraudulent employees. Additionally, companies must ensure that those who are fraudulent are identified and punished to prevent repeat offenses. By doing this, not only are they likely to hire employees with the right knowledge, but also those of good ethical character. By following these hiring guidelines, the potential for successful and high quality projects will undoubtedly increase.

REFERENCES

1. Associated Press, (2006 02 17). Radio Shack to close 400 to 700 stores. Retrieved November 28, 2006, from MSNBC.com Web site: <http://www.msnbc.msn.com/id/11409391/>
2. Chapman, Sandra (2004). Degrees of deception. Retrieved November 28, 2006, from WTHR - Indianapolis News and Weather Web site: <http://www.wthr.com/Global/story.asp?S=1854591>
3. Chapman, Sandra (2006). Government employees bought fake degrees. Retrieved November 28, 2006, from WTHR - Indianapolis News and Weather Web site: http://www.wthr.com/Global/story.asp?S=5532403&nav=menu188_2_2

4. ED.gov (2006). Accreditation fraud, abuse and related problems. Retrieved November 28, 2006, from U.S. Department of Education (Ed.gov) Web site: <http://www.ed.gov/about/offices/list/ous/international/usnei/us/edlite-accred-fraud.html#diplomamills>
5. Gasparino, Charles (2005 04 25). A criminal slips through. Retrieved November 28, 2006, from Newsweek Technology - MSNBC.com Web site: <http://www.msnbc.msn.com/id/7528899/site/newsweek/>
6. Mills, Ryan (2006 10 28). Officers fired for online degrees rehired. Retrieved November 28, 2006, from Naplesnews.com Web site: http://www.naplesnews.com/news/2006/oct/28/two_naples_officers_get_jobs_back/?local_news
7. OSAC, (2006 08 07). Want an "easy" college degree? Beware of illegal diploma mills!. Retrieved November 28, 2006, from Oregon Student Assistance Commission Office of Degree Authorization Web site: <http://www.ed.gov/about/offices/list/ous/international/usnei/us/edlite-accred-fraud.html#diplomamills>
8. Reuters, (2003 06 24). Microsoft ex-employee arrested for software theft. Retrieved November 28, 2006, from Yahoo! News India Web site: <http://in.tech.yahoo.com/030624/137/25eba.html>
9. The Standish Group (1994). The CHAOS Report. Retrieved September 11, 2006, from Sample Research - CHAOS Chronicles 1994. http://www.standishgroup.com/sample_research/chaos_1994_1.php
10. The Standish Group (2004). 2004 Third Quarter Research Report. Retrieved September 11, 2006, from Sample Research – Index. http://www.standishgroup.com/sample_research/PDFpages/q3-spotlight.pdf
11. UFL.com (2006). Is this Online Degree as Good as a Face-to-face Degree. Retrieved November 28, 2006, from University of Florida - Quality of a Degree Web site: <http://www.coe.ufl.edu/online/edtech/degreequality.htm>
12. USDOE-OPE, (2006 10). U.S. Department of Education Database of Accredited Postsecondary Institutions and Programs. Retrieved November 28, 2006, from US Department of Education - Office of Postsecondary Education Web site: <http://ope.ed.gov/accreditation/>
13. USNews.com (2006). America's best colleges 2007. Retrieved November 28, 2006, from USNews.com America's Best Colleges 2007: National Universities: Top Schools Web site: http://www.usnews.com/usnews/edu/college/rankings/brief/t1natudoc_brief.php
14. USAToday, (2006 02 20). Radio Shack CEO resigns amid resume questions. Retrieved November 28, 2006, from USATODAY.com Web site: http://www.usatoday.com/money/industries/retail/2006-02-20-radioshack-ceo_x.htm
15. Williams, Robert (2006 9 21). Braindumps, gunmen and cheaters. Retrieved November 28, 2006, from GoCertify.com Web site: <http://www.gocertify.com/article/braindumps.shtml>

NOTES