Educating The Next Generation Of Computer Security Professionals: The Rise And Relevancy Of Professional Certifications

James W. Gabberty, Pace University - New York, USA

ABSTRACT

This paper discusses the recent ascent and proliferation of computer security professional certifications. Based upon the premise that secure information technology not only underpins the current US economy but also represents a pivot point for future economic growth, it highlights the recent phenomenon of many information technology professionals complementing their Computer Science (CS), Information Systems (IS), and Information Technology (IT) degrees with highly specialized certification-based training to secure jobs that help to protect our national IT infrastructure. It also raises the question as to whether the trend of narrowly-focused specialized training signals a possible shift away from traditional academic computer security programs. If the present trend continues, the longer-term consequences for traditional academic degree programs could be dramatic. However, from the short-term perspective of this study, the proliferation of certification programs as a source of supplementary education is viewed as a positive phenomenon, helping to mitigate the disastrous effects associated with the continuous onslaught of domestic- and international-sourced cyber-attacks that threaten our national economic livelihood.

Keywords: Professional Certifications; Professional Education; Certification; Certification Programs

INTRODUCTION

There is no doubt that Information Technology (IT) has evolved to buttress the U.S. economy; any threats against this vital pillar may therefore poses serious consequences to our American way of life.

Ever since management guru Peter Drucker waxed prophetic more than fifty years ago about a future in which *knowledge workers*[1] would dramatically alter organizational structure, the sequencing of work and even corporate strategy, the world has witnessed the profound impact IT would have on economic growth (Drucker 1959). Subsequently, although there have been many studies that link IT to economic growth (Gabberty 1985; Brynjolfsson 1998), actually *proving* this well understood maxim has been all but impossible. This is so because of the way in which information technology expenditures are tracked by the Bureau of Labor Statistics, which collects information about the factors of production and correlates corresponding outputs that are used to compute the ratio commonly known as *productivity* (Jorgenson 2003). Irrespective of the methods used by the BLS to track IT expenditures and its cumulative effect on the economy, computing and information sciences has evolved to such an extent that nearly every aspect of modern society is somehow tied to technology and any disruptions to this vital infrastructure could seriously impact society.

[1] "Knowledge worker productivity is the biggest of the 21st century management challenges. In developed countries it is their first survival requirement. In no other way can the developed countries hope to maintain themselves, let alone to maintain their leadership and their standards of living."

The level of uncertainty that this infrastructural dependency carries with it has become manifest as vulnerabilities get exploited and network intrusion attempts skyrocket in frequency, challenging top administrators and industry leaders to question the overall stability of their respective infrastructures. The resulting need, and demand for well-trained, qualified information security (InfoSec) professionals will likely grow in lockstep with the rate of technological progress and cyber malfeasance. Similarly, the type of training that these professionals have obtained over the past decade and the kind they are likely to need is worthy of investigation. This leads to the question - 'to what extent are people receiving appropriate levels of InfoSec training, and can a trend be identified that points the way forward toward future educational programs?'

THE ILLUSORY NOTION OF IT-DRIVEN PRODUCTIVITY

Presently, the factors of production associated with IT (hardware, software, telecommunications gear, etc.) are not tracked with enough detail to enable accurate estimation of the contribution imparted by IT towards the nation's overall productivity. It is not surprising, therefore, that leading scholars and even a Nobel Laureate suggest that 'You can see the computer age everywhere but in the productivity statistics' (Solow 1987; Roach 1998; Gordon 2000; Kiley 2000).[2,3,4,5] In contrast, the public at large as well as many leading university researchers instinctively know that ever since the advent of networked personal computers, we have indeed entered a new era of *sustainable* economic growth driven by IT advances (DeLong 2002; Stiroh 2001) (emphasis added by the author). Unfortunately, and for causes that lie outside the domain of this paper, the IT profession has apparently lost some its attractiveness to college students and the long-term consequences that this loss of education cohorts will have on our national prosperity will not be measurable until the BLS updates the type of data it collects and the methodology it uses to process that data to yield productivity indices. Nonetheless, the upward levels of demand for qualified IT talent and shortages in [properly] trained talent not only lead to the outsourcing of potentially sensitive applications abroad, but also to a scarcity of information security talent that is necessary to deal with the dearth of network intrusion attempts and illegal hacking activity of private and public computers.

WHY THE IT PROFESSION (STILL) MATTERS

Although IT has been portrayed as having become somewhat of a commodity and in spite of the practical inability to directly link IT with economic progress and the causalities that drives away university students from completing college degrees in the computing sciences, few would argue that a secure IT infrastructure remains a critical component of the nation's overall economic well-being (Carr 2003). So while recent trends in employment are lackluster for most regions of the country, specialized sectors within the IT industry remain in high demand; jobs within these sectors are plentiful for those who possess proper credentials. This demand, as it turns out, has prompted professional organizations that provide timely, accurate and fast-paced learning programs with appropriate certifications to flourish.

[2] Robert Solow won the Nobel Prize in 1987 for his analysis of the sources of economic growth.

[3] Roach argued that IT-driven productivity revival is a statistical mirage due to the *understatement* of actual hours worked by IT workers, leading to *overstated* productivity growth.

[4] Robert Gordon argued that accelerated US productivity circa. 2000 was mostly due to cyclical forces.

[5] Michael Kiley argued that large IT costs may have actually *reduced* productivity growth.

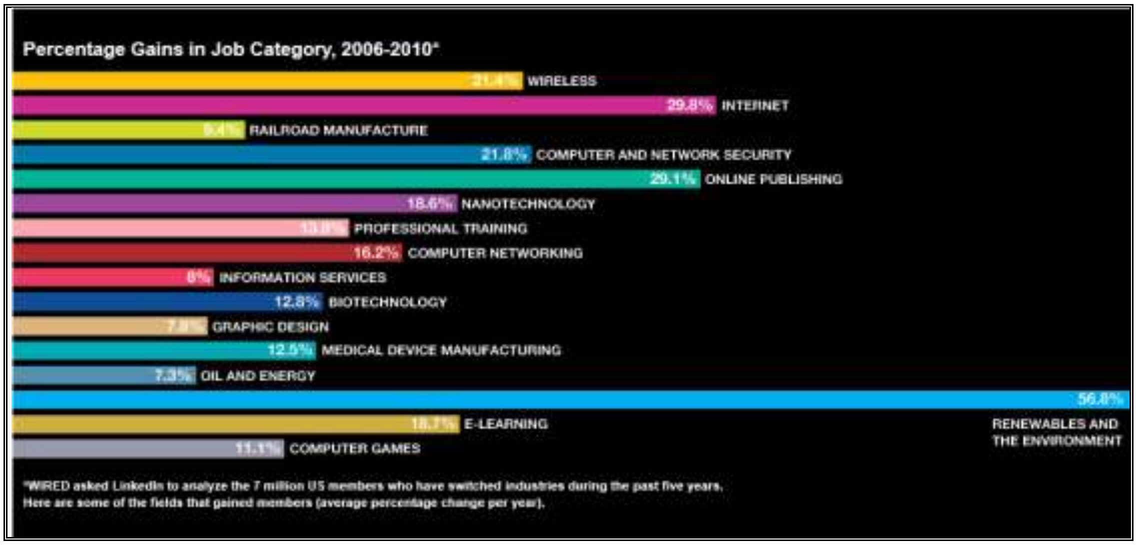

Figure 1 – Job Growth Rates in Selected Industries
Source: Where the Smart Jobs Are. *Wired*, June 16, 2011
Retrieved from http://www.wired.com/epicenter/2011/05/the-nerds-have-won/

A 2011 *Wired* magazine article entitled 'The Robots Haven't Won – 'Smart Job' Nerds Have", focuses on job sectors that exhibit double-digit growth (see Figure 1; Milikan 2011). Significantly, most of the high growth job categories are those in which information technology play a crucial role.[6] For technologists, the news gets even better: recent data by the U.S. Bureau of Labor Statistics identifies a potential growth rate of a whopping 34% having a median annual salary quartile value of 'Very High' for software and application engineers for the ten-year period 2008 through 2018.[7] If these numbers are anywhere near accurate, then individuals seeking employment in high-paying, established jobs should consider the IT sector as an attractive career path.

Why Specialize in Information Security?

While there are many specialties in IT that exhibit stellar growth, several particular disciplines stand out, one such example is the *Computer Security Specialist*[8], which boasts a career opportunity that is expected to 'grow rapidly' and 'projected to exhibit large numbers of job openings.'[9] Moreover, the U.S. Department of Labor ascribes the job prospects for *Computer Security Specialists* as having a 'Bright Outlook', which means that this occupation matches at least one of the following criteria: [10]

- Projected to grow much faster than average (employment increase of 20% or more) over the period 2008-2018,

[6] One particular sector – Renewables & the Environment – is cited as undergoing a 56.8% growth rate; it can be argued that that IT is part of the 'Green Movement' because of the way in which IT has been curbing its voracious appetite for [mostly] coal-fired electricity. At a June 2011 event held at the headquarters of Price Waterhouse Coopers in NYC (moderated by the author), IBM EVP David McCabe cited the massive reduction in greenhouse emissions that *could* be achieved by switching off millions of computers in the workplace and shifting data from local storage to Cloud storage as one of the reasons why IT can be viewed as a 'green' sector.

[7] Table 1.4 – "Occupations with the Largest Job Growth, 2008 and Projected 2018", Employment Projections Program, U.S. Department of Labor, U.S. Bureau of Labor Statistics. Retrieved from http://www.bls.gov/emp/ep_table_104.pdf.

[8] Defined by the U.S. Department of Labor as individuals who plan, coordinate, and maintain an organization's information security… [they] educate users about computer security, install security software, monitor networks for security breaches, respond to cyber-attacks, and, in some cases, gather data and evidence to be used in prosecuting cyber-crime. The responsibilities of computer security specialists have increased in recent years as cyber-attacks have become more sophisticated. Retrieved from http://www.bls.gov/oco/pdf/ocos305.pdf

[9] The Occupational Information Network (O*NET) is sponsored by of the US Department of Labor/Employment and Training Administration (USDOL/ETA) and as such, is the primary source of occupational information in the U.S. Retrieved from http://www.onetcenter.org/.

[10] Reference retrieved from http://www.onetonline.org/help/bright/15-1071.01

- Projected to have 100,000 or more job openings over the period 2008-2018, and
- Represents a 'New & Emerging' occupation.

Other related occupations assigned the moniker 'Bright Outlook' by the U.S. Department of Labor include *Security Management Specialists, Information Technology Project Managers, and Auditors.*[11,12,13]

Since the need for specialists in these particularly high growth industry professions is tied to the acceleration of security breaches and cyber-attacks, it is not surprising that the number of professionals who possess appropriate InfoSec certifications continues to grow. Further, Information Assurance, IT Enterprise Governance and IT Audit practitioners with the requisite certification are likewise in high demand as current and planned regulatory initiatives such as Sarbanes-Oxley and Dodd-Frank amplify the need for IA professionals to mitigate the harmful effects associated with fraud, information integrity and confidentiality breaches that belie these programs.

IT Security Practitioners Urgently Needed by the Military

From the perspective of the U.S. military, information security workers represent much more than basic levers of economic growth - they represent a crucial component of the nascent effort to defend the nation's information assets. With more than 90,000 full-time personnel maintaining the military's communications-based backbone (which consists of 15,000 networks and seven million computing devices dispersed globally) the scale of protecting these assets from cyber warfare threats that could wreak havoc on our national economy and potentially devastate our national security has increased dramatically (Lynn 2011).

Following the highly publicized information security breaches in our nation's public, private, government and military sectors, the U.S. military command found it necessary – despite being mired by a severe economic downturn – to establish the U.S. Cyber Command, which became operational in May 2010 (Gramone 2010). This command will counter the approximately 250,000 "Probes and scans" an hour that General Keith B. Alexander, commander, U.S. Cyber Command and director of the National Security Agency asserts challenge the U.S. computing infrastructure relentlessly and which has a five pillar strategy for operating in cyber space (Lopez 2010):

1. Treating cyberspace as an operational domain, like land, air, sea, and outer space;
2. Employing active defenses to stop malicious code before it affects our networks;
3. Protecting commercial networks that operate the critical infrastructure that our military relies upon;
4. Joining with allies to mount a collective cyber defense; and
5. Mobilizing industry to redesign network technology with security in mind.

The Nascent Field of Information Security

Given the dependency of our economy (and indeed, military infrastructure itself) on the continuous availability and flow of confidential and high integrity data, it is evident that the problems associated with [mostly] IP-based traffic disruptions can be likely countermanded by individuals possessing the kind of requisite skills that have over the past decade been made available by organizations offering specialized training and certification. But while the qualified organizations that provide this training are capable of keeping up with the rate of change of ever-morphing cyber-attack methods, academia moves at a much slower pace and in general, teaches basic IT tenets derived from often outdated textbooks as the main thrust of the content it delivers. As new attack vectors are unveiled, academia is simply not equipped to update its curricula to keep pace with these fast-moving events.

[11] Defined by the U.S. Department of Labor as individuals who conduct security assessments for organizations, and design security systems and processes; [they] may specialize in areas such as physical security, personnel security, and information security, and may work in fields such as health care, banking, gaming, security engineering, or manufacturing. Retrieved from http://www.bls.gov/oco/pdf/ocos305.pdf.

[12] Defined by the U.S. Department of Labor as individuals who examine and analyze accounting records to determine financial status of establishment and prepare financial reports concerning operating procedures; [they] are often required to possess a background in Computer Science & Accounting.

[13] Defined by the U.S. Department of Labor as individuals who plan, initiate, and manage information technology (IT) projects; [they] lead and guide the work of technical staff, serve as liaison between business and technical aspects of projects, plan project stages and assess business implications for each stage, and monitor progress to assure deadlines, standards, and cost targets are met.

Indeed, it was only as recent as 1988 when the Morris worm was coined as the first Internet-based exploitation by nefarious individuals seeking to wrest control over another computer. It is not surprisingly, therefore, that in this relatively short span of time that a universally-accepted, broad suite of up-to-date technical & managerial controls has not been developed and properly vetted by cadres of academic and professional practitioners. In other words, there is neither a single tome nor suite of texts that provides a *current* elixir to the perpetual onslaught of cyber attackers – there is instead a vast collection of InfoSec knowledge spread throughout the world, some of it codified and some of it passed on by an underground network of cyber criminals. And therein lays the problem: most academicians work in institutions that are just not set up to stay on top of zero-day exploits, develop taxonomies of attack vectors that reflect the state-of-the-art, and stay abreast of the enumerable IT vulnerabilities that seem to be always abundant. Instead, [we] academicians typically perform InfoSec research that generalizes the ‘big picture’, building theoretical models that lay the foundation for subsequent exploration by students and practitioners in the field. These models (cryptography comes to mind) can be heavily rooted in mathematics and fully understood oftentimes by a small cadre of academicians and InfoSec practitioners. Concomitantly, professional organizations often move more swiftly, speedily identifying and publishing new exploits and vulnerabilities, often providing quick-fixes and patches to mitigate losses while teaching abbreviated programs of course material that is often taught more comprehensively in academia (program and project management, for example).

The idea that academia is ‘mired in time’ at the dawn of the InfoSec (r)evolution is not at all unusual, especially when one considers how long it took for other well understood and universally accepted subjects to fully develop – each with their own principals and ideologies. What is unusual, however, is that while the InfoSec field continues to mature, successful intrusions nonetheless persist, culminating in losses of incalculable magnitude. Hence, the magnitude of the mission of U.S. Cyber Command and similar programs in the private sector become all the more sharply focused, and all the more urgent.

While what is known today about information security will eventually grow and most assuredly change, more academic research and time spent digesting the research findings are necessary for the natural evolution of the subject. This ‘maturation period’ can be better understood by examining similar lengthy cycles of maturation that other universally accepted and heavily vetted subjects (economics, management science and marketing, for example) endured before reaching their current state of evolution (which is *still* evolving). In these academic subjects, recent research has led to the over-turning of well-ensconced maxims that were replaced by newer theories decades, and even hundreds of years after their initial establishment. Several examples will clarify: *mobile* Labor and Capital (no longer seen as fixed assets) and their effect on economics, Virtual Teams and their impact on management, and Globalization & The Internet Economy and its effect on marketing all upset established dogma and resulted in a re-thinking of the foundations of these subjects. It is not hard to imagine a similar evolution for InfoSec field as it becomes more universally classified and organized.[14]

A look back several years after the advent of the Morris Worm provides further clues for the complexity of what once was an intermittent domestic problem but has become explosively more complicated as an unintended consequence of the Telecommunication Act of 1996. It is noteworthy to point out that this act, crafted to spur competition through convergence, was successful, but arguably became one of the causal factors for the explosive criminal activity that ensued soon after the Internet was opened up to commercial traffic [first domestically, then] around the globe. Roughly 15 years later, many millions of international-sourced probes into our military and civilian [re: commercial] computer networks has throttled-up the need to train individuals who can help thwart the mal-intent of agents behind these attacks.

With heightened demand for information security professionals both in the civilian and military sector, it would be logical to assume that the cohorts of students at colleges and universities offering computing and information sciences programs would be swelling, but according to the data, this is not the case. "The biggest challenge we currently face is generating the people we need to do this mission," says General Alexander, “My

[14] The birth of Economics is generally traced back to Adam Smith’s Wealth of Nations, which was first published in 1776 and the birth of Management Science is traced back to 1880 when Frederick W. Taylor began his famous “Time and Motion” in manufacturing

greatest concern is moving fast enough to provide a capability to defend our networks in time were a crisis to occur. We see that as our No. 1 mission - be ready" (Lopez 2010).

THE DECLINE OF ACADEMIC DEGREES IN COMPUTING

The need for trained IT professionals to staff the U.S Cyber Command and myriad private job openings in InfoSec couldn't be more at odds with recent global trends. At a time when academic degrees in Computer Science and Information Systems in the U.S. continue to decline, nations such as China and, to a lesser extent, India have been investing towards producing Computer Science and Engineering talent at an alarming pace. As many as 75,000 C.S. & Engineering collegiate-level degrees are awarded to people in China and 60,000 similarly trained in India *every* year (Anonymous 2010). To put that in contrast, consider that China and India combined produce [relatively inexpensive] computer scientists and engineers at a rate twice that of the U.S., furthermore, more than 50% of American engineering degrees are awarded to foreigners, mostly Chinese and Indians, a number that is not included in the doubling statistic.

The U.S., meanwhile, has seen a radical decline among B.S., M.S., and Doctoral degrees in Computer and Information Degrees (see Figure 2). In recent years, the numbers of bachelor's degrees conferred have followed patterns that differed significantly by field of study. While the number of bachelor's degrees conferred in the combined fields of engineering and engineering technologies increased 8 percent between 1998–99 and 2003–04, and then increased a further 8 percent between 2003–04 and 2008–09, some technical fields experienced a contrasting pattern. After an increase of 95 percent between 1998–99 and 2003–04, the number of baccalaureate degrees conferred in computer and information sciences decreased by 36 percent between 2003–04 and 2008–09.[15] Similar drops in master degree programs occurred as well, though for doctoral studies, the trend is somewhat opposite, but trivial since the smaller number of students enrolled in terminal study programs in the Computing and Information Sciences, are likely to enter the education sector (another 'Bright Outlook' career path).

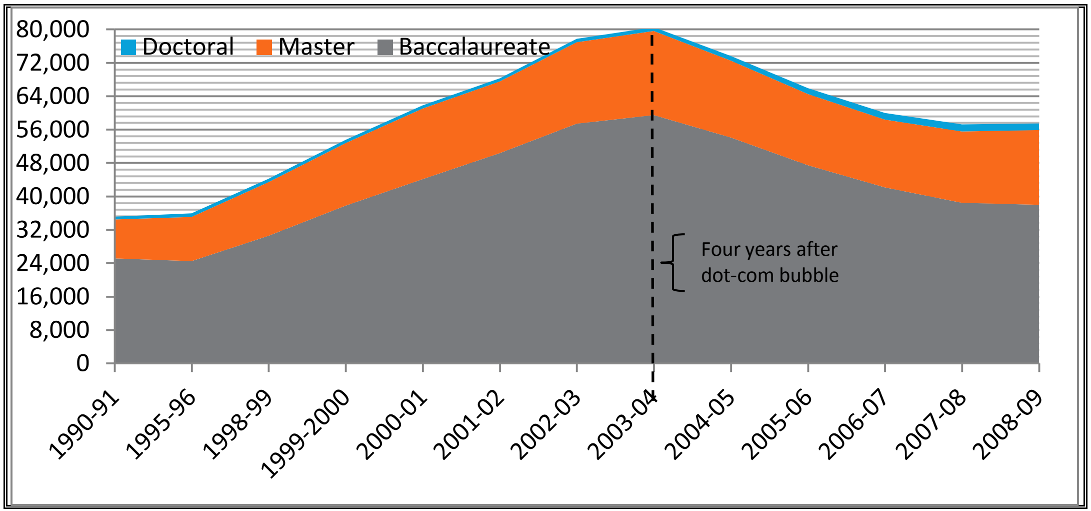

Figure 2 – Computer & Information Science Degree Conferrals
Source: U.S. Department of Education, Institute of Education Sciences, Tables 282, - 284 Bachelor's, Master's & Doctor's Degrees Conferred by Degree-Granting Institutions
Retrieved from http://nces.ed.gov/fastfacts/display.asp?id=37

So at a time when a larger, younger, and more sophisticated group of individuals should be poised to accept the mantle of responsibility passed on to them by the current crop of IT pioneers, recent trends show a woeful decline of suitably degreed IT would-be practitioners. This phenomenon ultimately begs the question, 'who is going to protect & defend our [inter]-national computing infrastructure, assuming many graduates in the field will bypass security and enter the application development side of the profession?'

[15] "Digest of Education Statistics: 2010 – Postsecondary Education", U.S. Department of Education Institute of Education Sciences. Retrieved from available at http://nces.ed.gov/programs/digest/d10/ch_3.asp

WHY CERTIFICATIONS MATTER

Jobseekers can enhance their employment opportunities by earning certifications, which are offered through product vendors, computer associations, and other training institutions. Many employers regard these certifications as the industry standard, and some require their employees to be certified. In some cases, applicants without formal education may use certification and experience to qualify for some positions. We do use a simple numbered heading scheme. In general, applicants with a college degree and certification will have the best opportunities. U.S. Department of Labor[16]

The gap created between the rigid, more formal education programs in computing & engineering sciences and the flexible, more state-of-the-art certification organizations is created by two factors: consistent technological advancement and the inability to keep up with this change. While some may point to the decline of the prestige of the engineering profession as primary cause, others lay blame on an education system that lags these technological advances. In either case, the risks associated with vulnerabilities continue to mount. Indeed, according to a recent study examining the shortage in the U.S. of skilled technicians in the manufacturing sector, nearly one-third of U.S. manufacturers report a shortage of skilled talent (Manyika, Pacthod and Park 2011).

One way to solve this burgeoning dilemma is, of course, to attract foreign nationals to *stay* in the U.S. after completing their programs of study rather than returning back to their home countries, where they pursue work and compete directly against the U.S. in all sectors. This solution is tricky, because it calls for a loosening of H-1 and B-3 visas (presently capped at 65,000, and as high as 195,000 in 2003) and its restrictive policies that were immediately put in place after the 911 attacks as a protective measure against further assaults on the U.S. and its vital infrastructure.

Table 1 – Pros and Cons of Academic vs. Professional Education

Qualitative Assessment Of Information Security Programs: Academic Vs. Professional Certification Programs		
Academic Degree Programs		
Benefit	• Contextual learning	Non-IT courses often complement major program of study
	• Universal curricula	Enables students at academically accredited schools to transfer between colleges & universities
	• Program material vetted	Material presented often fully developed and researched
Drawback	• Workforce entry delays	Pace of learning not set by student - course availability & scheduling conflicts extends program
	• Content becomes 'stale'	Some course content not updated to keep pace with rate of change of technology
Professional Certification Programs		
Benefit	• Workforce entry expedited	Program flexibility enables students to 'work & learn'
	• Certification widely accepted	Strict auditing of certification agencies by ANSI ensures compliance with rigid program standards
	• Material content often developed & delivered by industry practitioners	Relevancy, currency, and accuracy of presented material means students get exposed to state-of-the-art practices
Drawback	• Non-transferability of courses to academia	Dis-similar accrediting agencies, program length and textbooks means students can have difficulty transferring certifications into colleges & universities
	• Research often not vetted in peer-reviewed journals	Affiliates of certification agencies typically do not publish in academic, peer-reviewed journals
	• Few instructors possess Ph.D. or equivalent in CS or IS	Lack of terminal 'in-field' degree can mean limited exposure to theoretical constructs, resulting in loss of seeing the 'big picture'

[16] "Computer Network, Systems, and Database Administrators" in Occupational Outlook Handbook, 2010-11 Edition, U.S. Dept. of Labor, Bureau of Labor Statistics. Retrieved from available at http://www.bls.gov/oco/ocos305.htm

Another potential solution is that of renewing efforts by the private sector to train, develop, and retain engineering talent, though this solution can be problematic given our economic condition. Still another potential solution is that offered by the U.S. Department of Labor's High Growth Job Training Initiative, which targets 14 key sectors for investments in workforce development, of which Information Technology occupies one of the fourteen slots. Several years ago, the Employment and Training Administration (ETA) convened an IT Industry Executive Forum at CompTIA Headquarters in Oakbrook Terrace, Illinois, at which executives representing 18 companies from sectors such as IT hardware, software, cross-industry end users, and service providers discussed a wide range of workforce issues concerning the information technology industry, including the role for government in the IT industry's workforce initiatives, the need to develop the workforce soft skills, transferable IT skills, and the development of an industry competency model.[17] Among the set of workforce solutions that came out of that meeting, one stark statistic arose: over 90% of IT workers are performing jobs outside the IT industry.[18] This talent pool represents a highly capable cadre of individuals who, through InfoSec retooling & retraining, could make an impact on our nation's infrastructural vulnerability.

Even though the ETA emphasized the urgency for this large block of talent to receive IT training and complementary training in non-InfoSec for-profit sectors such as health care, manufacturing, and financial services, it can be argued that this cadre of workers (or some subset of them) would be well advised to pursue careers in information security and information security management. One such way to accomplish this is through professional certification because an assumption can made that the vast majority of them already possess college degrees of one pedigree or another.

Table 1 illustrates several of the predominant themes associated with certification programs in comparative context with academia, which often takes longer to yield qualified, employable graduates. In contrast, professional certification organizations prepare practitioners for employment opportunities at a much faster rate, with arguably near or advanced preparedness parity.

Professional Certification Agencies as Guilds

Upon graduation from prestigious universities such as MIT, Stanford, Harvard, etc., graduates enjoy the benefits associated with alumni services that offer lifelong benefits resulting from their association with their Alma Mater. This means that the school not only provides academic learning and formal degrees, but additional non-tangible benefits such as the prestige of having graduated from a top tier university, numerous job prospect opportunities, occasions to participate in high quality symposia at little or no cost, and continued contact (if desired) between the school and the individual to track their career progression. For most colleges however, this post graduate relationship does not exist, and more often than not attempts to reach graduates after they depart the institution are few and far between, the exception being an annual plea for alumni donations.

In contrast, professional credentialing organizations typically take measures to remain in contact with graduates, bolstering the depth, breadth (and value) and the education they provided. Further, certification agencies continue the learning process by establishing communities of interest that meet virtually from time to time (weekly and/or monthly) via online webinars and other open meetings, and by providing access to continually-updated research that active members can access anytime they want.

In this sense, the behavior of the credentialing agencies to act as 'guilds' or communities of interest is different from the traditional college experience because they strive to increase the value (and relevancy) of their education by promoting social networking among peers – leading to self-identity of members, learning, enhanced reputation, and in general, some aspect of income smoothing (similarly credentialed individuals often share data about prospects of their profession, including estimates of billing rates that are more or less in line with similarly credentialed professionals.

[17] U.S. Department of Labor report entitled "Statewide Solutions to Address Information Technology Industry Workforce Needs". Retrieved from http://www.doleta.gov/BRG/Indprof/IT.cfm.
[18] Ibid.

Why Certifications Are Highly Valued by InfoSec Professionals

In addition to the academic rigor provided by colleges and universities, studies by non-profit and for-profit firms alike reinforce the benefit derived by information security professionals who add a professional certification to their bona fides, as previously discussed. In sum, professional certifications provide individuals with additional tangible and intangible benefits as a result of their certification process, as outlined in a parallel study predicting the future of work (Malone 2004). These include:

- *Marketable* skills that cover both the technology and managerial perspectives (in contrast to technical degrees, which often omit managerial training),
- *Status of affiliation* that demonstrates 'dedication to the art' through continued learning,
- *Satisfaction of job requirements* that mandate that future jobs be offered to professionals with specialized certifications and that present job holders receive training for continued employment in their respective jobs,
- *Tacit knowledge* learned through codified pedagogy,
- *Peer-to-peer mentoring* (as opposed to 'lecturer-listener' model typified throughout academia where many instructors are not practitioners but instead rely on textbooks to impart knowledge,
- *Hands-on training and exposure to best-of-breed* as defined by current InfoSec practitioners, and
- *Code of ethics enforcement* whereby certifications may be revoked if transgressions warrant (as opposed to academic degrees that are left intact when transgressors bring shame on themselves and their industries (Worldcom and Enron come to mind).

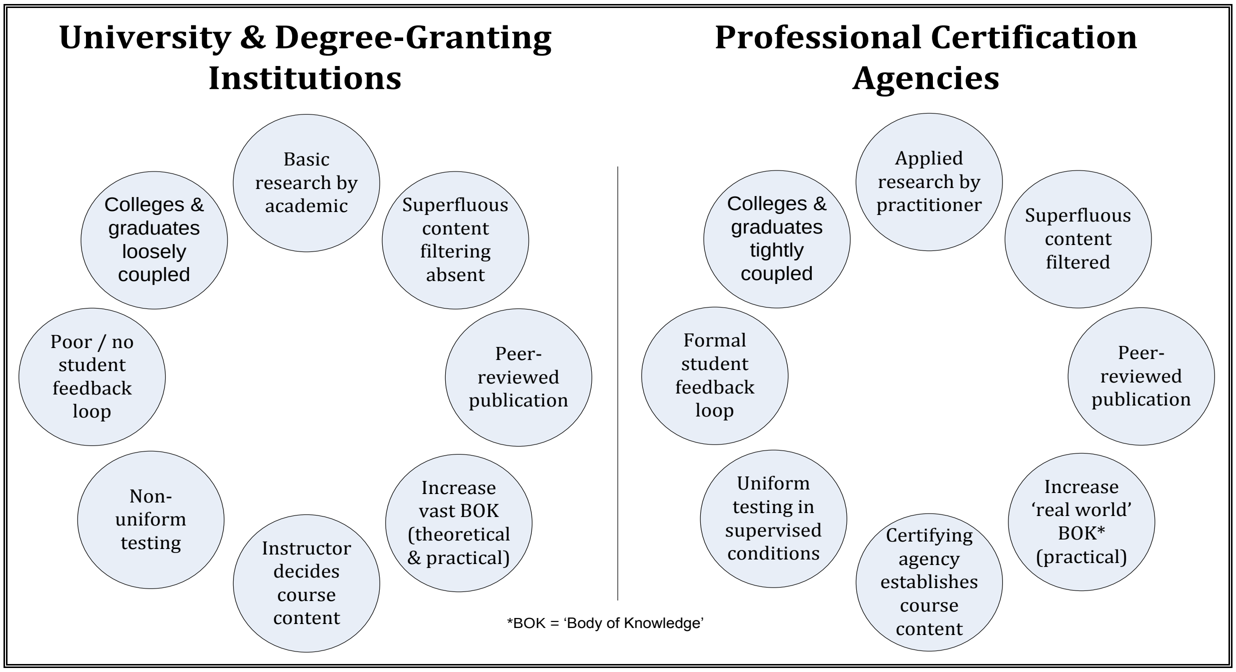
University & Degree-Granting Institutions
Basic research by academic
Colleges & graduates loosely coupled
Superfluous content filtering absent
Poor / no student feedback loop
Peer-reviewed publication
Non-uniform testing
Increase vast BOK (theoretical & practical)
Instructor decides course content
Professional Certification Agencies
Applied research by practitioner
Colleges & graduates tightly coupled
Superfluous content filtered
Formal student feedback loop
Peer-reviewed publication
Uniform testing in supervised conditions
Increase 'real world' BOK* (practical)
Certifying agency establishes course content
*BOK = 'Body of Knowledge'

Figure 3 – Pedagogy Development in Academia and Professional Certification Institutions

Table 3 provides an overview of the basic differences in pedagogy that exists in academia and professional certification companies, and may be useful for those considering acquiring InfoSec certification.

ACCREDITATION OF COMPUTING TECHNOLOGY CERTIFICATION ORGANIZATIONS

Before selecting a professional organization that provides swift and stimulating training and certification, individuals would be wise to recognize the value imparted by the supra-national organizations that assess and confirm the viability of their overall programs and validity of their certifications. The primary reason why professional organizations opt to have their certifications validated by federal and international agencies such as the American National Standards Institute (ANSI) and the International Standards Organization (OSI) is because these agencies distil (global) expertise and sound practices by people who understand the problems and are best placed to observe the standards in action and to maintain them as the state of the art.[19] Of the dozens of InfoSec certification organizations that open themselves up to inspection by these validating agencies, only a handful of these organizations have invested the time and money needed for the rigorous examination of their curricula. As such, those certifications that have received accreditation by these agencies are held in much higher regard, both in academia and in private industry.

Table 2– Information Security & Management Certificating Agencies

ANSI/ISO/IEC 17024 Accredited Certification Organizations	
Agency	**Certified Program Name**
Global Information Assurance Certification (GIAC)	• Certified Forensics Analyst (GCFA) • Certified Incident Handler (GCIH) • Certified Intrusion Analyst (GCIA) • Security Essentials Certified (GSEC) • Security Leadership Certification (GSLC)
Information Systems Audit & Control Association (ISACA)	• Certified in the Governance of Enterprise IT (CGEIT) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA)
International Information Systems Security Certification Consortium, Inc. (ISC)^2	• Certified Information Systems Security Professional (CISSP) • Certification and Accreditation Professional (CAP) • Certified Secure Software Lifecycle Professional (CSSLP) • Information Systems Security Architecture Professional (ISSAP) • Information Systems Security Engineering Professional (ISSEP) • Information Systems Security Management Professional (ISSMP) • Systems Security Certified Practitioner (SSCP)

ANSI / ISO / IEC Standards

ANSI makes the claim that it is the only personnel certification accreditation body in the United States that meets nationally accepted practices for accreditation bodies.[20] Hence, one of ANSI's most important functions is accreditation. ANSI accredits standards developers, certification bodies and technical advisory groups (TAGs) to both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).[21] Another such (international) organization, the ISO, for example, collaborated with its partners in international standardization, namely, the IEC (International Electrotechnical Commission) and the ITU (International Telecommunication Union), particularly in the field of information and communication technologies, to establish the World Standards Cooperation (WSC) as a focal point for their combined strategic activity.

[19] ISO in Brief – International Standards for a Sustainable World. *International Standards Organization*. Retrieved from http://www.iso.org/iso/isoinbrief_2011.pdf

[20] Accreditation Services, American National Standards Institute. Retrieved from https://www.ansica.org/wwwversion2/outside/PERgeneral.asp?menuID=2

[21] "ANSI Accredited Programs", American National Standards Institute. Retrieved from http://www.ansi.org/about_ansi/accredited_programs/overview.aspx?menuid=1

To ensure conformity among organizations providing audit and certification of management systems, ISO & IEC established the ISO/IEC 17011 standard, which codifies how this conformity is achieved. ANSI leveraged the ISO/IEC 17011 standard to develop ANSI/ISO/IEC 17024, the Accreditation Program for Personnel Certification Bodies. Figure 4 lists representative InfoSec members and the specific certifications they offer that are accredited by ANSI. Key points regarding ANSI accreditation are:

- ANSI accreditation includes site visits to ensure that compliance with requirements; ANSI accreditation is generally recognized as the highest standard in personnel certification accreditation
- The standard used by ANSI to accredit certification bodies is an American National Standard as well as an ISO/IEC Standard. This is extremely useful for companies with global operations or aspirations
- ANSI follows an internationally recognized process for accrediting organizations. This International Standard recognizes ANSI accreditation in any multilateral and/or mutual recognition agreements.

Brief overviews of the professional organizations that have secured accreditation by ANSI/ISO are presented in the following sections.

GIAC Certification Program

GIAC is an acronym for Global Information Assurance Corporation. It was founded in 1999 to validate the real-world skills of IT security professionals. GIAC's purpose is to provide assurance that a certified individual has practical knowledge and skills in key areas of computer security. GIAC offers certifications for job-specific responsibilities that reflect the current practice of information security. GIAC is unique in measuring specific knowledge areas of general purpose information security knowledge. GIAC certifications are classified in the following subject areas: Security Administration, Management, Audit, and Software Security.

ISACA Certification Program

ISACA got its start in 1967, establishing auditing controls in computer systems that were becoming increasingly critical to the operations of their respective organizations. In 1969, it incorporated itself as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.

ISACA publishes a technical journal in the information control field, the ISACA Journal. It hosts a series of international conferences focusing on both technical and managerial topics pertinent to the IS assurance, control, security and IT governance professions.

(ISC)^2 Certification Program

The International Information Systems Security Certification Consortium, Inc., (ISC)^2, educates and certifies information security professionals throughout their careers. (ISC)^2's mission is to make society safer by improving productivity, efficiency and resilience of information-dependent economies through information security education and certification. (ISC)^2 develops and maintains the (ISC)^2 CBK, a compendium of information security topics. The CBK is a critical body of knowledge that defines global industry standards, serving as a common framework of terms and principles that their credentials are based upon and allows professionals worldwide to discuss, debate, and resolve matters pertaining to the field. Subject matter experts continually review and update the CBK.[22]

[22] Data gleaned from corporate website - 'About (ISC)'. Retrieved from https://www.isc2.org/aboutus/default.aspx

The Ascent of Certifications in Information Security

Although a handful of organizations such as ISACA have developmental roots in the 1960s, many of today’s professional organizations were founded since the Internet became commercially available on a worldwide basis. Their genesis stemmed from the need for a new channel of education that was needed to counter the rising misconduct of cyber deviants and criminals.

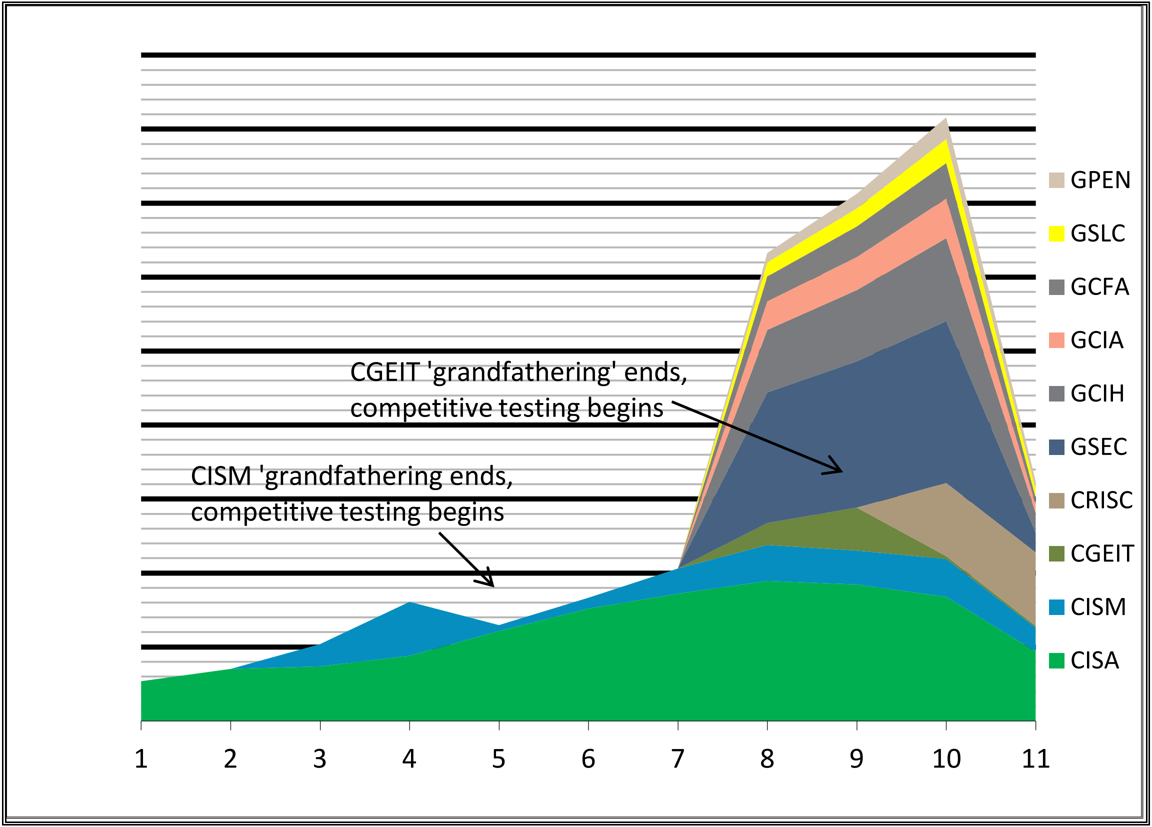

Figure 4 – Certifications Conferred for Selected Years
Source: Information Systems Audit & Control Association (ISACA), GIAC

The dramatic uptake by students (see Figure 4) of certifications offered by these organizations contrasts sharply with the downward trend associated with computing and information science degrees conferred over the past half-decade. [It should be noted that the figure is somewhat distorted because the data used to draw the figure includes partial data for the year 2011 and needs to be updated after the 2011 certifications counts are completed.] Nonetheless, their upward trend seems to indicate that these organizations, which have embraced online education and testing, are viewed as successful job-certifying organizations.

Moreover, the attention they pay to network intrusions and exponentially-growing attack profiles is impressive, so even though many network intrusions (successful or otherwise) do not get picked up by the media, in many instances they do get noticed and listed by these organizations, which subsequently publicize the nefarious activities that occur regularly. The group Anonymous, for example, a civil-disobedience group (whose only membership requirement is the ability to conceal one’s online identity) has gained public notoriety as a result of its piracy and ‘hacktivist’ network intrusion activities. The level of attention Anonymous has received in recent months may be responsible for spawning even wider interest among would-be InfoSec practitioners as well as by the companies that employ them. In sum, the reasons why InfoSec certifications have become so popular are many, but certainly is related to the enlarged employment opportunities that await them after proper training and certification is achieved.

CONCLUSION

The challenges for today’s information security worker associated with maintaining currency in software administration & security, audit, forensic, managerial and legal domains are not unlike those who pioneered earlier infrastructure layouts such as the telephone and internal combustion engine, except for the pace at which the digital infrastructure becomes stabilized. For earlier infrastructure advancements, technological improvements arrived quickly and the problems associated with deploying them were remedied quickly. The Internet, and the machinery that drives it, will likely remain unstabilized (re: vulnerable) for some time to come, a reflection that the TCP/IP protocol suite was developed without security in mind. Computing speeds, bandwidth, and storage innovations will propel the Internet faster and faster as adoption by commercial businesses, governments, and the militaries of the world leverage these advances in newer, more novel ways. This ‘competitive intensity’ (which has more than doubled in the past 40 years) offers productivity, efficiency and creativity advantages that are limited only by the minds of the pioneers who continue to evolve the shape, reach and speed of our digital infrastructure (Hagel III, Brown and Davison 2009).

Estimates vary, but according to one source, our digital infrastructure created 150 exabytes (billion gigabytes) in 2005 and last year, that number grew to 1,200 exabytes (Anonymous 2010). Undoubtedly, some of this data is poised to enter the Cloud, where (presumably) it will be secure. But for the rest of this information residing outside the Cloud, the resulting risk arising from this data explosion lies in myriad social security numbers, tax data, credit card numbers and other personal information that drives continued security breaches, ID theft and fraud.

The threats that loom over our digital infrastructure will multiply, further pushing-up risk levels associated with calamitous security breaches. So, at least for the foreseeable future, professional certifications earned by the modern InfoSec professional will help to stem the tide of ever-mounting encroachment attempts, at least until academia eventually figures out a way to speed up its sometimes outmoded approach to teaching.

In the meanwhile, cutting the gap between the speed of digital progression and compensatory education for today’s professional information security worker is what drives organizations such as GIAC, ISACA and (ISC)^2. So while academia struggles to maintain relevancy in the IT security arena, the supplemental training by these professional organizations will undoubtedly flourish, as will the demand for professionals who possess both an academic degree and one or more certifications from these accredited institutions. It may be concluded that pursuing professional certifications amplify the likely success of professional InfoSec practitioners. Meanwhile, as for academia, it can learn much from its supplemental pedagogy cousin, perhaps taking action to foster ties and joint research that will benefit all. For the professional certification agencies, possible actions might include establishing links to more serious academic peer-reviewed journals through co-authorship of research papers, co-teaching opportunities, and consideration to accept certifications as proof positive that students enrolled in these institutions might receive transfer credits to satisfy part of an academic degree program of study. An action item for degreed CS and IS individuals, certainly, is to consider adding as many professional certifications as they can to their toolkit because by doing so, they will have demonstrated a dedication to the art that is sometimes lacking in information technology circles; a side benefit will be likely boost to their prospects of finding a satisfying career trajectory. That said, we can only hope that in the race to protect our collective digital infrastructure that the call to arms is heard - and responded to - by all.

AUTHOR INFORMATION

James W. Gabberty is professor of information systems at Pace University's Seidenberg School of Computer Science and Information Systems in New York and an alumnus of the Massachusetts Institute of Technology and New York University Polytechnic Institute. He has served as an expert witness in telecommunication & information security at the federal and state levels, and holds numerous post-doctorate certifications management, innovation and technology. Dr. Gabberty has more than thirty years of experience as a consultant to Wall Street and has witnessed first-hand the dramatic impact that technological change has caused for the global financial services industry. He is the author of numerous articles on the innovative uses of information and communication technology, the impact of e-commerce, and competitive advantage of nations. E-mail: jgabberty@pace.edu

REFERENCES

1. Anonymous (April 17, 2010). A World Turned Upside Down – A Special Report on Innovation in Emerging Markets, *The Economist*, p. 4.
2. Anonymous (February 27, 2010). The Data Deluge. *The Economist*, p. 11.
3. Brynjolfsson, Erik and Lorin M. Hitt (1998). Beyond the Productivity Paradox: Computers are the Catalyst for Bigger Changes. *Communications of the ACM*, 41(11).
4. Carr, Nicholas G. (2003). IT Doesn't Matter, *Harvard Business Review*, 8(5).
5. DeLong, J. Bradford (2002). *Do We Have a "New" Macroeconomy?*, Cambridge, National Bureau of Economic Research, MIT.
6. Drucker, Peter (1997). *Management Challenges for the 21st Century*, Oxford, Butterworth-Heinemann.
7. Gabberty, James W. (1985). The Proliferation of the Computer in American Business, *Engineering Management Review*, IEEE, December.
8. Gordon, Robert J. (2000). Does the 'New Economy' Measure Up to the Great Inventions of the Past?. *Journal of Economic Perspectives*, 14(4), Fall.
9. Gramone, Jim (2010). Alexander Details U.S. Cyber Command Gains. *American Forces Press Service*, September 24. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=61014
10. Hagel III, John, Brown, John Seely, and Lang Davison (2009). The Big Shift – Measuring the Forces of Change. *Harvard Business Review*. July-August, 87:7-8.
11. Jorgenson, Dale (2003), *Productivity: Information Technology and the American Growth Resurgence*, Cambridge, MIT Press.
12. Kiley, Michael T. (2000). Computers and Growth with Frictions: Aggregate and Disaggregate Evidence. *Federal Reserve Board*, Mimeo, October.
13. Lopez, C. Todd (2004). Building Work Force Top Challenge for Cyber Command. U.S. Army report. September 24. Retrieved from http://www.army.mil/article/45658/Building_work_force_top_challenge_for_Cyber_Command/
14. Lynn, William J. III (2010). Defending a New Domain - The Pentagon's Cyberstrategy. *Foreign Affairs*, September-October.
15. Malone, Thomas W. (2004). *The Future of Work.* Cambridge, Mass: Harvard Business Press.
16. Manyika, James, Pacthod, Daniel, and Michael Park (2009). Translating Innovation Into US Growth. *McKinsey Quarterly*, May citing (2009) People and Profitability: A Time for Change - A 2009 People Management Practices Survey of the Manufacturing Industry. Deloitte, Oracle, and the Manufacturing Institute.
17. Milikan, Arikia (2011). The Robots Haven't Won – 'Smart Job' Nerds Have. *Wired*, May 3. Retrieved from http://www.wired.com/epicenter/2011/05/the-nerds-have-won
18. Roach, Stephen S. (1998). No Productivity Boom for Workers. *Issues in Science and Technology*, IV(4), Summer.
19. Solow, Robert S. (1987). We'd Better Watch Out. *New York Times (Book Review)*, July 12.
20. Stiroh, Kevin J. (2001). Information Technology and the U.S. Productivity Revival: What Do the Industry Data Say?. Federal Reserve Bank of New York paper. The Federal Reserve. Retrieved from: http://ideas.repec.org/p/fip/fednsr/115.html