How secure is education in Information Technology? A method for evaluating security education in IT

Mark Grover
mjgrover@us.ibm.com
Technical Enablement Specialist, Watson University
IBM Watson Group Durham, NC

Bryan Reinicke
breinicke@saunders.rit.edu
Department of MIS, Marketing and Digital Business
Rochester Institute of Technology
Rochester, NY 14623

Jeff Cummings
cummingsj@uncw.edu
Information Systems and Operations Management
Dept. University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

As the popularity of Information Technology programs has expanded at many universities, there are a number of questions to be answered from a curriculum standpoint. As many of these programs are either interdisciplinary, or at least exist outside of the usual Computer Science and Information Systems programs, questions of what is appropriate for the curriculum and accreditation have arisen. More specifically, as the demand for information security professionals has expanded enormously, IT majors will increasingly be asked to fill these roles. This paper seeks to examine the curriculum for IT programs with a special focus on security. Security has become an increasingly important topic, and one that IT graduates will likely be dealing with professionally. We answer this question by examining the curriculum guidelines for IT programs, and comparing these to both professional standards and IT program curriculums at several universities.

Keywords: IT Education; Curriculum; Accreditation; Security; Certification.

1. INTRODUCTION

The Need for Information Security

The demand for Information Security professionals is at an all-time high, yet there is no readily available research outlining specific education deliverables within an Information Technology curricula to prepare students. A study found that the demand for cybersecurity professionals over the past five years grew 3.5 times faster than for other IT jobs (Vijayan, 2013). The Bureau of Labor and Statistics predict information security analyst jobs to grow 22% from 2010 to 2020 (U.S. Department of Labor, 2013). Not only is the demand increasing but salaries for security professionals are typically higher than others in IT. Robert Half Technology's 2015 Salary Survey shows a network security administrator can expect to earn between $99,250 and $138,500 and a data security analyst can expect to earn between $106,250 and $149,000 annually (Robert Half Technology, 2015).

In May 2009, President Barack Obama identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation" (Obama, 2009). Since then many schools and universities have begun to offer varying degree programs that focus on Information Security; however, the education delivered at each is quite different. Unlike a math or accounting degree, where there is an acceptable standard by which to measure one school to another, there is no set standard for information security.

Since starting this research in 2013, multiple groups have met to discuss the learning outcomes for Cyber-related educational offerings. One provider of curricula recommendations is the Association for Computing Machinery (ACM). ACM regularly publishes curricula recommendations for Computer Science and Information Technology programs. As of this writing, the most recent Information Technology curriculum guideline for undergraduate programs was published in November 2008 (Association for Computing Machinery, 2015).

Other groups such as the Cyber Education Project (CEP) have formed to develop curriculum guidelines for a "Cyber Science" degree track (Cyber Education Project, 2015). What these groups have in common is the desire to create curricula that meets accreditation standards. However, curricula at various universities need to be explored to understand if these programs are meeting the guidelines outlined for successful security programs.

Our study is designed to evaluate IT programs to understand if these are meeting the needs of the security field. The following questions are evaluated in the subsequent sections:

- Are curricula at various universities covering the guidelines set out for security education?
- Furthermore, do these guidelines meet the needs of employers based on their measures of qualifications (e.g., certifications)?

2. LITERATURE REVIEW

It is clear that education is key to obtaining a job as a security professional. The 2013 IT Salary Survey on Security performed by InformationWeek shows that 99% of participants indicated they had completed at least some higher education or tech school classes, as shown in **figure 1** (All of the tables and figures for this study are presented in **Appendix 1**) (Lemos, 2013). According to the Bureau of Labor and Statistics, "Information security analysts usually need at least a bachelor's degree in computer science, programming, or a related field" (U.S. Department of Labor, 2013). This is supported by a survey of 682 IT Security professionals (Lemos, 2013). Of those who responded, between 77% and 78% of respondents had a Bachelor's degree or higher (see Figure 1). Additionally, higher education can also serve as a substitute for experience, as some job postings mention that education can be utilized in lieu of experience. In the subsequent sections, security in education will be discussed and expanded on. This is followed by expanding the discussion of education into the area of certifications.

Security in Education

To address the need for some common understanding about cybersecurity, the National Institute of Standards and Technology (NIST) was tasked with creating a cybersecurity framework. The result was the National Initiative for Cybersecurity Education (NICE). "The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security" (National Institute of Standards and Technology, 2011). The NICE framework was designed to help map course work to a predefined set of knowledge, skills, and abilities (KSAs). The framework addresses what skills are needed for various types of jobs; however, it does not provide specifics on what education and certifications are required to obtain the necessary skills. This framework was used by the ACM as a starting point for the development of curriculum guidelines for universities (McGettrick, 2013). This suggests the ACM guidelines provide a sufficient measure universities can use to understand if their curriculum is meeting the needs of employers seeking cybersecurity professionals. However, this may not be the lone measure to assess curricula.

On November 19th and 20th, 2013, the inaugural Cyber Education Symposium was hosted in Arlington, VA. The event featured representatives from industry, government, and education in a panel format to discuss how to better prepare a cybersecurity workforce. The various panels met to discuss challenges and spoke in very abstract terms about educational requirements. The last plenary panel consisted of Robert Hutchinson, Sandia National Labs; Albert Palacios, the Department of Education; Evan Wolff, Crowell & Moring; and Tom Baughan, Monster.com. The entire panel was asked to give their opinions as to what specific education they wanted to see out of two- and four-year graduates. The answers given were still very abstract. At the conclusion, a few members suggested that certifications are currently how many representatives from the various industries assess the security education of potential employees. This is similar to how the Department of Defense and other government agencies currently handle education in which they have specific requirements for Information Assurance workers including both training and certifications (for more information, see DoD 8570 for a list of certifications required by federal employees).

Certifications are often used as a bar for employers to understand if job candidates have the knowledge needed for a position in security. Because higher education is meant to develop students ready for the workforce, it would be helpful to understand if the current guidelines set out by ACM and adopted by universities meet the knowledge and skills tested through certification. Thus, in the subsequent section, certifications are discussed and the skills/knowledge gained through these certifications are compared to the current IT curriculum guidelines.

The Value of Certification

Certifications offer a standardized way in which employers can assess future employees. From the previously referenced survey of IT professionals, the following question was posed to understand the value of education/training (e.g., certifications) for security professionals: "What type of training would you find most valuable to you in developing your career?" (Lemos, 2013). The answers given to this question provides an honest assessment of where the participants feel they need to improve (see **Figure 2**). Note that certification courses rate as one of the top two considered most valuable in further developing a security career, only slightly behind the need for technology-specific training. A recent study of government workers found that "staff members holding certifications make $12,000 more and managers make $10,000 more in base salary than their noncertified counterparts" (Ballenstedt, 2013).

According to the 2013 and 2014 US IT Salary Surveys of IT security staff and management professionals performed by InformationWeek, more than 60% of those surveyed have at least one security certification. The same surveys also provided statistics about the effect security certifications have on compensation. Certification attributes to an average increase in total compensation of over $9,000 (Lemos, 2013).

Another survey found that "a $21,000 boost in salary can be yours if you obtain Certified Information Systems Security Professional (CISSP) or two other major security certifications" (Brodkin, 2008). The article cited research by Foote Partners, an IT research and advisory firm that monitors compensation of IT professionals.

The review of both guidelines and certification suggest there are a variety of approaches to security education. Based on this, it is clear there needs to be a set of standards that properly equips a cybersecurity workforce. There is consensus that certain jobs require specific certifications. But are we preparing our students to fill these needs? Do our curriculum guidelines match up with the skills that our employers are demanding? Furthermore, are the guidelines set out by ACM and used by most universities aligning with skills and knowledge tested through certifications?

In the subsequent section, we first evaluate ACM guidelines on IT curricula at various universities. We then expand on these ACM guidelines by comparing them to the most popular certifications in security related fields to understand if these guidelines meet the skills/knowledge set by these certifications.

3. METHODOLOGY

To understand how universities are currently incorporating security into their curriculum, a qualitative study examining current information technology curriculum was performed. Evaluating all programs in Information Technology was beyond the scope of this research. Instead, this research evaluates the Information Technology degree programs within the University of North Carolina education system. This provided a smaller set of universities to help in developing a guideline to evaluate other universities in multiple states.

The evaluation is based on the established curriculum and accreditation guidelines for this area. The University of North Carolina education system (UNC System) consists of "16 university campuses across the state" (University of North Carolina, 2015). To ensure similar programs are evaluated, Classification of Instruction Programs (CIP) codes are utilized. CIP was "developed by the US Department of Education's National Center for Education Statistics in 1980 for the accurate tracking and reporting of fields of study and program completions activity" (US Department of Education: Institute of Education Sciences, 2015). For this research, the Information Technology programs with a CIP code of 11.0103 were evaluated. All the schools within the UNC System are accredited by the Southern Association of College and Schools (SACSCOC, 2014). The schools with an IT degree program are shown in Table 1 (in Appendix).

Once each school with a qualifying program was identified, required core classes and electives were evaluated. The purpose of this research is not to compare a given program to another, but rather focuses on the required core classes that include security, and any security related electives offered. In order to identify classes that include security, the search terms "security", "secure", "crypto", "assurance", "intrusion", and "protect" were used. These terms were selected after a pre-evaluation of the course catalogs of the schools evaluated, and were then verified by four subject matter experts as being an appropriate grouping of words to demonstrate courses falling under the security umbrella. This included two faculty currently teaching in the security curriculum and one industry expert. Each university's course catalog was searched and classes that matched these keywords were added to the analysis.

Utilizing the keywords resulted in a reduced chance of overlooking a course that delivers security related content; however, each catalog was reviewed fully for any additional security class offerings. The results from this are shown in Tables 2 and 3. While evaluating the curriculum at each UNC System school, an effort was made to determine if a certification is currently a deliverable. Of the classes evaluated, there was no mention of any requirement for a certification as a class prerequisite, or requiring certification for class completion.

Guidelines and Certification Comparisons

First, courses were compared to the elements set out by the ACM IT IAS guidelines (Association for Computing Machinery, 2015). These guidelines set out 11 knowledge areas (KAs) that are suggestions of topics to be covered as well as time to be given to each topic. Each knowledge area contains various components of specific topics that will be compared to courses currently being offered in IT curricula.

Next, an analysis of the CISSP, Security+, and CEH certifications was performed, breaking the body of knowledge for each certification into its component parts. These certifications were chosen based on an evaluation of jobs currently available in security, and the certifications most commonly identified as being required/preferred (see Figure 3). This information was collected through a search of the Dice.com employment database for the term "security analyst" limited to include only Georgia, South Carolina, North Carolina, and Virginia. Forty-four of the 60 jobs returned, or 73%, had a Bachelor's degree listed as either preferred or required. Forty-one of the 60 jobs had either a required or suggested minimum experience listed. Of those with a required minimum, 32 of them required five years or less experience.

The search also revealed 60% had some form of certification requirement or recommendation. The most popular certification requested was CISSP, with Security+, Certified Information Systems Auditor (CISA), and Certified Ethical Hacker (CEH), all tied for second. Further evaluation of these four certifications revealed that the CISA certification concentrates on auditing, and has a five year minimum experience requirement, so it was not evaluated as part of this research.

Common elements from each certification were identified, and then evaluated by the subject matter experts to ensure the elements were appropriately classified. Once these were confirmed, the elements were then used to evaluate the classes being taught. The goal is to create a list of required elements of security that should be taught, yet be certification neutral. This is referred to as the recommended body of knowledge. These were then compared to the current knowledge areas that encompass the ACM curricula guidelines to assess if these guidelines cover the recommended body of knowledge from certifications. Lastly, the opposite is compared in which certifications are evaluated against the ACM guidelines to understand if certifications encompass these guidelines. The content of each class was compared to the recommended body of knowledge to see how many elements are being fulfilled. Once each class had been evaluated, each University program was evaluated, based on its fulfillment of the recommended body of knowledge.

4. RESULTS

Are the courses covering the Material?
The first evaluation was made by looking at the curriculum in the UNC IT programs and comparing it to the key elements of the ACM guidelines. Table 2 shows the university, degree program and the courses offered that have a required security element. The courses listed are broken out by whether they are required for IT majors, or are elective courses. The analysis for this study focuses on the required courses, as students may or may not take a given elective.

Table 3 shows the required courses at each school that contain a key security element identified by the ACM. Table 4 shows how these key elements map to the ACM IT guidelines. Table 5 reflects a summary of a detailed evaluation of each required and elective classes offered in Information Technology curriculum programs within the UNC System and shows that all the elements of the ACM IT IAS guideline KA's are being taught in required courses. It can also be seen from the data, however, that not every school is covering every element of the curriculum in required classes. This finding is hardly surprising, given that the curricula vary between schools.

Does ACM = Certifications?
The next question this study set out to answer was: Are the ACM Guidelines covering skills required by the popular certifications? In order to measure this, the study compared the detailed elements of the ACM IAS with the three certifications identified as the most popular (CISSP, Security+ and Certified Ethical Hacker). The comparison of the certifications is shown in table 6. This table maps the elements of each certification to those identified by the ACM, with references to the section of the certifications guides where that knowledge area can be found. It is interesting to note that none of the certifications covers all of the areas of the ACM guidelines.

The next question is, do the ACM guidelines cover all aspects of the security certifications? In order to answer this question, a similar analysis was preformed, but in reverse. Each certifications knowledge areas were listed and mapped against the ACM guidelines.

CISSP was the most commonly listed certification in job postings, so we begin there. Table 7 shows, in summary, that the ACM guidelines do not cover all of the knowledge areas required by this certification. While all of the areas are covered at least partially, the coverage varies from 25-75%. In particular, CISSP requires more in the area of secure development and what could be viewed as the "managerial" aspects of security, such as risk management and asset security. The fact that the ACM guidelines miss so many of the "managerial" aspects of security is particularly troubling, as these make up the majority of cyber security best practices (Kleinberg, Reinicke and Cummings 2015).

Table 8 shows that the ACM guidelines cover 100% of the knowledge areas required by the Security+ certification. This is perhaps not surprising, as the Security+ certification is a more general certification than the others listed here. However, it also indicates that an IT degree program that follows the ACM guidelines will by default prepare its students for this certification.

The final certification examined in this study is the Certified Ethical Hacker (CEH). The comparison of the CEH to ACM guidelines is presented in table 9. Here the ACM guidelines cover from 0-100% of the knowledge areas listed by the certification. This is an interesting finding, and serves to highlight the fact that the CEH is a very detailed, technical certification. This particular certification goes into great depth on every area of hacking, which is very unusual to find in academic programs, because it is so specific.

Do Certifications = ACM?
The next analysis performed was to measure the percentage of the ACM guidelines covered in the knowledge areas of each of the certifications. A summary of this comparison is found in table 10. Once again, we can see that the overlap with the Security + certification is the highest, at 100% for all of the knowledge areas.

However, while the ACM guidelines do not fully cover the CISSP and CEH certifications, neither do these certifications cover all of the ACM guidelines. The reverse coverage is significantly better for the CISSP, ranging from 64-100%. That is to say, the knowledge areas from the CISSP more fully reflect the ACM guidelines, which shows that the certification covers more areas overall than the ACM guide. Again, this is not a surprise as the CISSP is a specialized

certification that would go into more depth than a general IT program would be expected to.
Finally, the CEH covers between 0 and 100% of the ACM knowledge areas. Once again, this is not surprising as the CEH is a very in depth technical certification, which is not designed to cover all aspects of IT education.

Recommendations

Based on the comparison of the ACM IT guidelines and the requirements of the three certifications examined, it is clear that there is a great deal of overlap. In practical terms, this means that those programs following the ACM recommendations for their IT programs are covering the majority of what the students would see on some of the more general security certification exams.

This same analysis, though, points out that more attention needs to be paid to the managerial aspects of security. While it is possible that some of these items are covered in courses that were not specifically security classes, and did not appear on our analysis, it seems likely that more attention needs to be paid to this area.

Finally, this analysis shows an academic program will be hard pressed to prepare its students for a more technical certification exam, like the CEH. These certifications are very technical and specific in nature. It could be argued that it is inappropriate for a general degree program to prepare students for something like this. It could, however, be possible for a program to create a specialized track that would prepare students for the CEH while covering the broader topics required by the ACM in other courses.

Limitations

This study looked only at schools within the UNC system. In addition, not all of the IT programs were considered. Only those coded the same in the system were compared for consistencies sake. The study did not have access to the syllabi for all of the courses listed in each of these programs, so the assessment was based upon the catalog descriptions. As technology classes tend to evolve more quickly than university catalogs, it is possible that the courses cover topics other than those listed in the descriptions.

This study also did not look at elective courses within the programs. While there may be additional security topics covered in elective courses, there is no way to ensure that all students take a particular elective. As the purpose of the study was to see how the base curriculum compared with the requirements in security, only those courses were examined.

Another limitation included only examining the ACM curriculum guidelines along with a limited number of certifications. We chose these guidelines as they provide a general overview of Information Technology curriculum that many universities are trying to incorporate into their curriculum. There are a number of additional resources (e.g. Cyber Education Project) that can be used for future examination.

Finally, this study looked only at the University of North Carolina system. As such, it is difficult to draw conclusions nationally with this study. However, the study does provide a method for evaluation of programs in other states.

Future Work

This study could be expanded to other states to examine IT education in those areas of the country. This could also be expanded to include the elective courses offered within a program to see if a student could fulfill all of the requirements for the security certifications by taking additional coursework. Finally, it may be beneficial to examine all course in IT programs to make suggestions as to where security to be included to help prepare students for the security field.

5. CONCLUSIONS

This research does not attempt to settle the debate of whether certifications should or should not be a deliverable in an educational setting. However, it is clear that a properly delivered security minded curricula does provide a solid foundation for at least two of the top three certifications identified in this research, namely Security+ and CISSP.

The research also demonstrates that there is a wide variation in the amount of time spent on security education in different schools. This is certainly understandable, but points to a problem moving forward. As security becomes more critical in an ever more connected society, educating technology professionals on security becomes crucial. This is far from an insurmountable problem – it simply requires a reexamination of course material to include security where applicable.

The ACM IT Curricula Guidelines used in this research are just that, guidelines. It was not intended to be a mandatory implementation list. This research has shown that there is a demand for individuals who are experts in security. This shows that there are synergies for those programs that more closely follow the guidelines. An effective implementation of these guidelines will fulfill both the educational mission of the university and provide the skills required by employers.

6. REFERENCES

Association for Computing Machinery. (2015, January 12). Curricula Recommendations. Retrieved January 12, 2015, from Association for Computing Machinery: Advancing Computing as a Science & Profession: http://www.acm.org/education/curricula-recommendations

Ballenstedt, B. (2013, April). Cybersecurity Jobs Continue to Pay Better Than Others. Retrieved November 30, 2013, from *Nextgov*: http://www.nextgov.com/cio-briefing/wired-workplace/2013/04/cybersecurity-jobs-continue-pay-premium/62485/

Brodkin, J. (2008, June 11). Salary boost for getting CISSP, related certs. Retrieved from *NetworkWorld*: http://www.networkworld.com/article/2280774/lan-wan/salary-boost-for-getting-cissp--related-certs.html

Kleinberg, H., Reinicke, B. & Cummings, J. (2015). "Cyber Security Best Practices: What to do?" *Journal of Information Systems Applied Research*, 8(2), 52-59.

Lemos, R. (2013, January). Research: 2013 Salary Survey: Security. Retrieved from *InformationWeek* Reports: http://reports.informationweek.com/abstract/166/10337/Professional-Development-and-Salary-Data/Research:-2013-Salary-Survey:-Security.html

McGettrick, A. (2013, August 30). Toward Curricular Guidelines for Cybersecurity. *Association for Computing Machinery*, pp. 1-33. Retrieved February 4, 2015, from http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

National Institute of Standards and Technology. (2011, September 19). *National Initiative for Cybersecurity Education* (NICE). Retrieved November 30, 2013, from http://csrc.nist.gov/nice/aboutUs.htm

Obama, B. (2009, May). The Comprehensive National Cybersecurity Initiative. Retrieved November 30, 2013, from The White House: Foreign Policy: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Robert Half Technology. (2015). Robert Half Technology 2015 Salary Guide. Retrieved June 6, 2015, from Salary Guide and Salary Center: http://www.roberthalf.com/salary-guides

SACSCOC. (2014, December 20). Commission on Colleges: Search Results. Retrieved December 20, 2014, from Southern Association of Colleges and Schools Commission on Colleges: http://www.sacscoc.org/search.asp

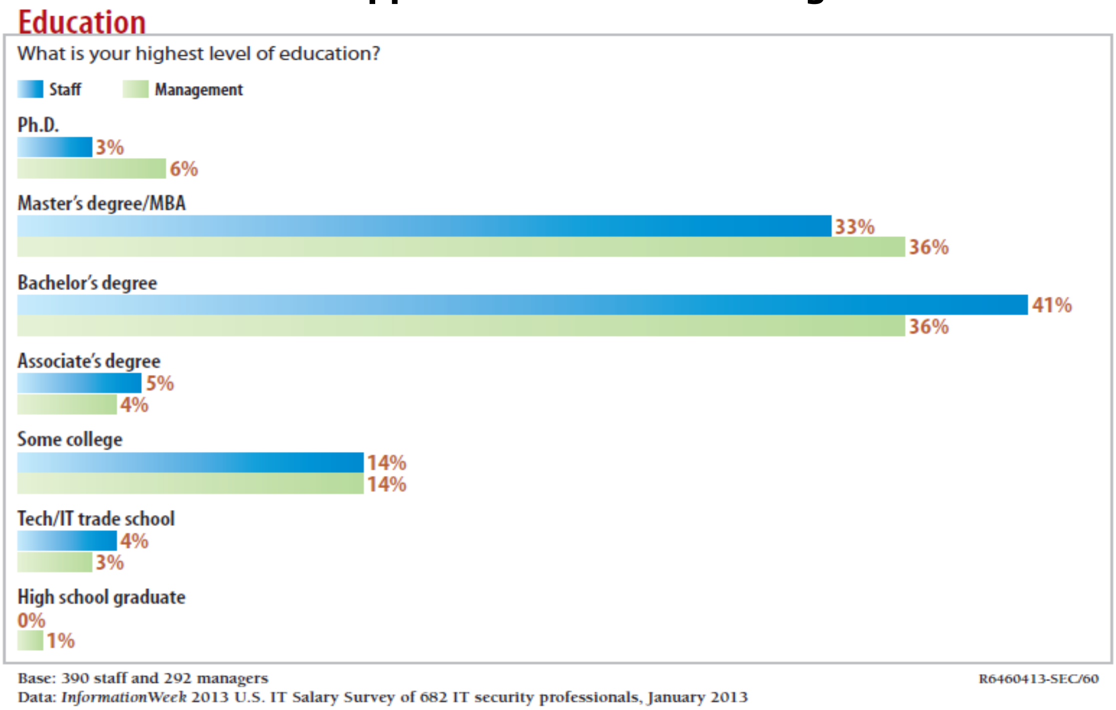
University of North Carolina. (2015, January 30). About Our System. Retrieved January 30, 2015, from University of North Carolina: A System of Higher Learning: http://www.northcarolina.edu/?q=content/about-our-system

US Department of Education: Institute of Education Sciences. (2015, January 12). What is CIP? Retrieved January 12, 2015, from *Classification of Instructional Programs* (CIP): http://nces.ed.gov/ipeds/cipcode/Default.aspx?y=55

U.S. Department of Labor. (2013, November 30). Occupational Outlook Handbook, 2012-13 Edition, Information Security Analysts, Web Developers, and Computer Network Architects, Retrieved from *Bureau of Labor Statistics:* http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm

Vijayan, J. (2013). Demand for IT security experts outstrips supply. Retrieved November 30, 2013, from *Computerworld*: http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply

Appendix 1: Tables and Figures



Education

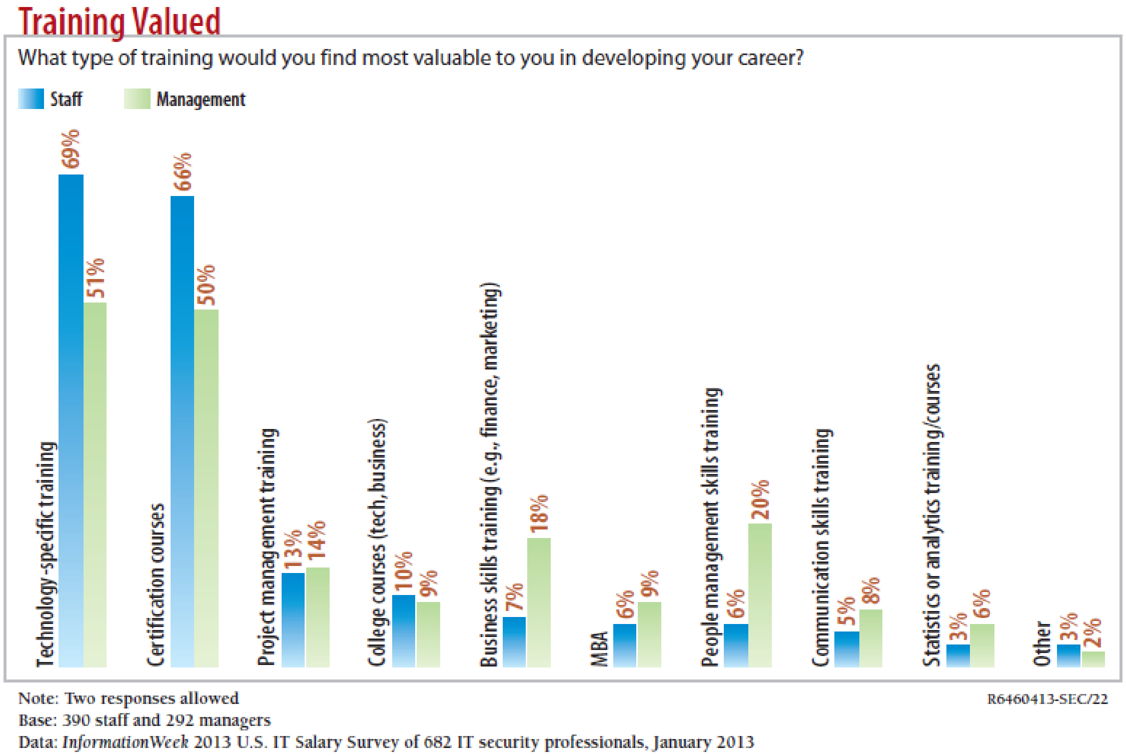
What is your highest level of education?

Base: 390 staff and 292 managers

Data: *InformationWeek* 2013 U.S. IT Salary Survey of 682 IT security professionals, January 2013

R6460413-SEC/60

Figure 1 – Education level held by participants (Information Week 2013 Salary Survey)



Training Valued

What type of training would you find most valuable to you in developing your career?

Note: Two responses allowed

Base: 390 staff and 292 managers

Data: *InformationWeek* 2013 U.S. IT Salary Survey of 682 IT security professionals, January 2013

R6460413-SEC/22

Figure 2 – Security, Most Valuable Training (InformationWeek 2013 Salary Survey)

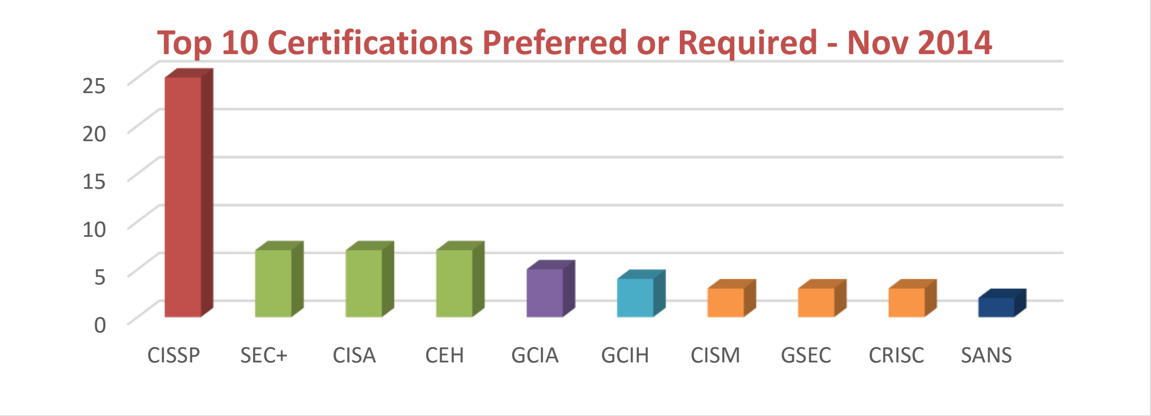


Figure 3 – Certifications preferred of required based on November 2014 Job Listings

	CIP	Information Technology			Accreditation (ABET, 2015)
		BS	MS	PhD	
East Carolina University	11.0103	X			
NC A&T State University	11.0103	BS in Information Technology program starting Fall 2015[1]			
UNC Charlotte	11.0103		X		
UNC Pembroke	11.0103	X			
UNC Wilmington	11.0103	X			
Winston-Salem State University	11.0103	X			ABET: IT,BS 2011-Present

Table 1 – UNC System Schools with an IT degree program

CIP Code	UNC School	Degree	Required Security Classes	Security Electives
11.0103	East Carolina University	BS IT	ICTN 4200, 4201, 4800, 4801	
11.0103	UNC Charlotte	MS IT	ITIS 6200	ITIS 5220, 5221, 5250, 6150, 6167, 6210, 6220, 6230, 6240, 6362, 6420
11.0103	UNC Pembroke	BS IT	ITC 2080	ITC 3250
11.0103	UNC Wilmington	BS IT	CIT 204, 324, 410, 213	
11.0103	Winston-Salem State University	BS IT	CSC 3325	

Table 2 – Information Technology classes with a security component

Key Security Element	Distribution		
Database	CIT 213 (UNCW)		
Information, Privacy & Security	ITIS 6200 (Charlotte)	CSC 3325 (Winston)	
Intrusion Detection	ICTN 4200 (ECU)	ICTN 4201 (ECU)	
Information Assurance	ICTN 4800 (ECU)	ICTN 4801 (ECU)	
Systems Administration	ITC 2080 (Pembroke)		
Digital Media	CIT 204 (UNCW)		
Info. Sec. Management	CIT 324 (UNCW)		
Web App. Development	CIT 410 (UNCW)		

Table 3 – Distribution of Information Technology Required Classes with a Security element

Key Security Element Being Taught	Most Closely Maps to ACM IT Guideline
Database	IAS/Security Domains

[1] http://www.ncat.edu/academics/schools-colleges1/sot/index.html, January 30, 2014

Key Security Element Being Taught	Most Closely Maps to ACM IT Guideline
Information, Privacy & Security	IAS/Fundamental Aspects, IAS/Security Mechanisms, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities
Intrusion Detection	IAS/Attacks, IAS/Vulnerabilities
Information Assurance	IAS/Fundamental Aspects, IAS/Security Domains, IAS/Information States, IAS/Security Services
Systems Administration	IAS/Information States
Digital Media	IAS/Security Mechanisms, IAS/Forensics, IAS/Information States
Info. Sec. Management	IAS/Fundamental Aspects, IAS/Operational Issues, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities
Web App. Development	IAS/Attacks, IAS/Vulnerabilities

Table 4 – Information Technology security elements being taught mapped to ACM IT IAS guidelines

UNC School	Degree	KA's Fulfilled (max 11)	% ACM IT IAS Guideline being delivered. (KA's offered / 11 KA's)
East Carolina University	BS	6	55%
UNC Pembroke	BS	5	45%
UNC Wilmington	BS	11	100%
Winston-Salem State University	BS	7	64%
UNC Charlotte	MS	11	100%

Table 5 – Evaluation of Information Technology Degrees with required and elective courses that include security elements compared to ACM IT IAS guide line

ACM IAS Guideline for Information Technology	CISSP	Security+ SY0-401	CEH 312-50
1. IAS/Fundamental Aspects [3 hours]			
1.1 History and terminology	Throughout	Throughout	Throughout
1.2 Security mindset	Throughout	Throughout	Throughout
1.3 Design principles	3.A-E	1.3	1.6
1.4 System/security life-cycle	7.E	4.1	-
1.5 Security implementation mechanisms	3.A-E	2.9	1.2
1.6 Information assurance analysis model	3.B	3.6	1.1
1.7 Disaster recovery	6.C	2.8	-
1.8 Forensics	7.A	2.4	-
2. IAS/Security Mechanisms			

ACM IAS Guideline for Information Technology	CISSP	Security+ SY0-401	CEH 312-50
2.1 Cryptography	2.E / 3.E,I / 4.A	6.1-3	19.1-8
2.2 Authentication	5.A-B, E	5.1-3	1.6 / 5.4
2.3 Redundancy	7.K	2.8	-
2.4 Intrusion detection	7.C,H	3.6 / 4.3	17.1-2
3. IAS/Operational Issues			
3.1 Trends	-	2.6	1.1
3.2 Auditing	6.E	2.3	20.1
3.3 Cost/benefit analysis	1.G	2.8	1.3
3.4 Asset management	7.D	2.7 / 4.2-3	-
3.5 Standards	1.F / 2.E	2.1-2	-
3.6 Enforcement	8.B	2.3 / 2.5	-
3.7 Legal issues	1.D	4.2	-
3.8 Disaster recovery	6.C	2.8	-
4. IAS/Policy			
4.1 Creation of policies	1.F	2.1	1.6
4.2 Maintenance of policies	1.F	2.1	1.6
4.3 Prevention	1.J	2.7	1.6
4.4 Avoidance	1.J	2.7	1.6
4.5 Incident response (forensics)	7.G	2.4	1.6
4.6 Domain integration	7.D	1.1-2 / 2.7	1.6
5. IAS/Attacks			
5.1 Social engineering	1.J	3.3	9.1-6 / 2.3
5.2 Denial of Service	7.H	3.2	10.1-8
5.3 Protocol attacks	4.A	3.2	8.1 / 8.4
5.4 Active attacks	-	3.7	5.4 / 8.1
5.5 Passive attacks	-	3.7	5.4 / 8.1
5.6 Buffer overflow attacks	8.B	3.5	13.2 / 13.5 / 14.1-9 / 18.1-7
5.7 Malware	7.H	3.1	6.1-7 / 7.1-6
6. IAS/Security Domains			
6.1 Security awareness	1.L	1.4 / 2.2	1.1 / 13.1-2
7. IAS/Forensics			
7.1 Legal systems	2.F / 7.B	2.4	-
7.2 Digital forensics and its relationship to other forensic disciplines	7.A	2.4	-
7.3 Rules of evidence	7.A	2.4	-
7.4 Search and seizure	2.F / 7.B	2.4	-

ACM IAS Guideline for Information Technology	CISSP	Security+ SY0-401	CEH 312-50
7.5 Digital evidence	7.A	2.4	-
7.6 Media analysis	2.A / 7.A / 7.F	2.4	-
8. IAS/Information States			
8.1 Transmission	4.B	4.4	-
8.2 Storage	4.B	4.4	-
8.3 Processing	4.B	4.4	-
9. IAS/Security Services			
9.1 Confidentiality, Integrity, Availability	1.A / 3.A	2.9	1.1
9.2 Authentication	5.A-B, E	5.2	1.6 / 5.4
9.3 Non-repudiation	3.I	2.9 / 6.1	1.1
10. IAS/Threat Analysis Model			
10.1 Risk assessment	1.I	2.1 / 4.5	-
10.2 Cost benefit	1.I	2.1	-
11. IAS/Vulnerabilities			
11.1 Perpetrators	1.J	3.2-5	1.3
11.2 Inside attacks	1.J	3.2-5	9.2
11.3 External attacks	1.J	3.2-5	1.3
11.4 Black hat	-	3.8	1.3
11.5 White hat	-	3.8	1.3
11.6 Ignorance	-	3.8	-
11.7 Carelessness	-	3.8	-
11.8 Network	4.D	1.5 / 3.4,6	3.1-2
11.9 Hardware	7.D	4.3	5.4
11.10 Software	8.B	4.1	5.4
11.11 Physical access	7.O	2.7,9	-

Table 6 – Mapping ACM 2008 IT Curricula Guidelines and security certification requirements

CISSP Domains	% KA's Linked to ACM IT IAS Guideline
Security & Risk Management (CISSP Domain 1) – 12 KA's	58%
Asset Security (CISSP Domain 2) – 6 KA's	50%
Security Engineering (CISSP Domain 3) – 11 KA's	54%
Communication & Network Security (CISSP Domain 4) – 4 KA's	75%
Identity and Access Management (CISSP Domain 5) – 7 KA's	43%
Security Assessment and Testing (CISSP Domain 6) – 5 KA's	40%
Security Operations (CISSP Domain 7) – 16 KA's	63%
Software Development Security (CISSP Domain 8) – 4 KA's	25%

Table 7 - Percent of CISSP Domain KA's linked to ACM IAS Guideline

Security+ Domains	% KA's Linked to ACM IT IAS Guideline
Network Security (Security+ Domain 1) – 5 KA's	100%
Compliance and Operational Security (Security+ Domain 2) – 9 KA's	100%
Threats and Vulnerabilities (Securtiy+ Domain 3) – 8 KA's	100%
Application, Data, and Host Security (Security+ Domain 4) – 5 KA's	100%
Access Control and Identity Management (Security+ Domain 5) – 3 KA's	100%
Cryptography (Security+ Domain 6) – 3 KA's	100%

Table 8 - Percent of Security+ Domain KA's linked to ACM IAS Guideline

Certified Ethical Hacker Modules	% KA's Linked to ACM IT IAS Guideline
Introduction to Ethical Hacking (CEH Module 1) – 6 KA's	67%
Foot printing and Reconnaissance (CEH Module 2) – 6 KA's	17%
Scanning Networks (CEH Module 3) – 2 KA's	100%
Enumeration (CEH Module 4) – 11 KA's	0%
System Hacking (CEH Module 5) – 4 KA's	25%
Trojans and Backdoors (CEH Module 6) – 7 KA's	100%
Viruses and Worms (CEH Module 7) – 6 KA's	100%
Sniffers (CEH Module 8) – 9 KA's	22%
Social Engineering (CEH Module 9) – 6 KA's	100%
Denial of Service (CEH Module 10) – 8 KA's	100%
Session Hijacking (CEH Module 11) – 5 KA's	0%
Hacking Webservers (CEH Module 12) – 8 KA's	0%
Hacking Web Applications (CEH Module 13) – 7 KA's	43%
SQL Injection (CEH Module 14) – 9 KA's	100%
Hacking Wireless Networks (CEH Module 15) – 9 KA's	0%
Hacking Mobile Platforms (CEH Module 16) – 8 KA's	0%
Evading IDS, Firewalls and Honeypots (CEH Module 17) – 8 KA's	25%
Buffer Overflows (CEH Module 18) – 7 KA's	100%
Cryptography (CEH Module 19) – 8 KA's	100%
Penetration Testing (CEH Module 20) – 6 KA's	17%

Table 9 - Percent of CEH Module KA's linked to ACM IAS Guideline

ACM IT IAS Guideline	% of ACM IT KA's Tested		
	CISSP	Security+ SY0-401	CEH 312-50
IAS/Fundamental Aspects	100%	100%	63%
IAS/Security Mechanisms	100%	100%	75%
IAS/Operational Issues	88%	100%	38%
IAS/Policy	100%	100%	100%
IAS/Attacks	71%	100%	100%
IAS/Security Domains	100%	100%	100%
IAS/Forensics	100%	100%	0%
IAS/Information States	100%	100%	0%
IAS/Security Services	100%	100%	100%
IAS/Threat Analysis Model	100%	100%	0%
IAS/Vulnerabilities	64%	100%	73%

Table 10 – Percent of ACM IT Guidelines covered by popular certifications