THE SANS 2005-2007 INFORMATION SECURITY SALARY & CAREER ADVANCEMENT SURVEY

What factors impact compensation?

Which security certifications matter?

What makes security people mad?

What matters for career advancement?

Updated July 10, 2007

Executive Summary

More than 4,250 security professionals participated in the 2005 Information Security Salary and Career Advancement Survey, conducted between October 20 and November 18, 2005. They provided detailed answers to thirty questions about their compensation, their background, their employer, their certifications, their job responsibilities and satisfaction and what it takes to get promoted. This executive summary provides a top level view of (I) employer and employee factors that impact security professionals' salaries, (II) how certifications impact salaries and technical job performance, (III) what it takes to satisfy security workers and (IV) what critical skills are necessary for professional advancement.

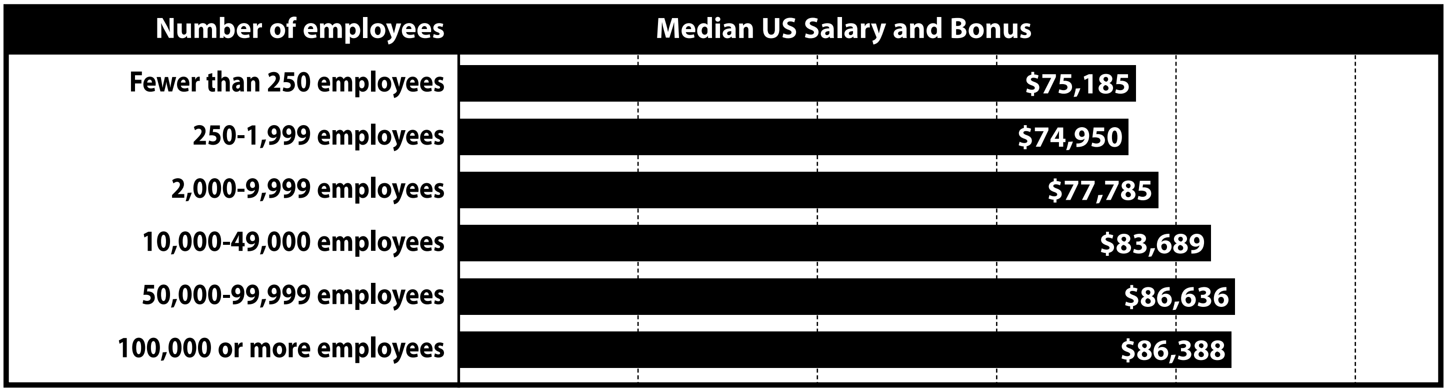
The complete survey data can be found in the 18-page report, which is available to current SANS students who e-mail salary@sans.org.

Section I. Compensation and the Factors That Impact It

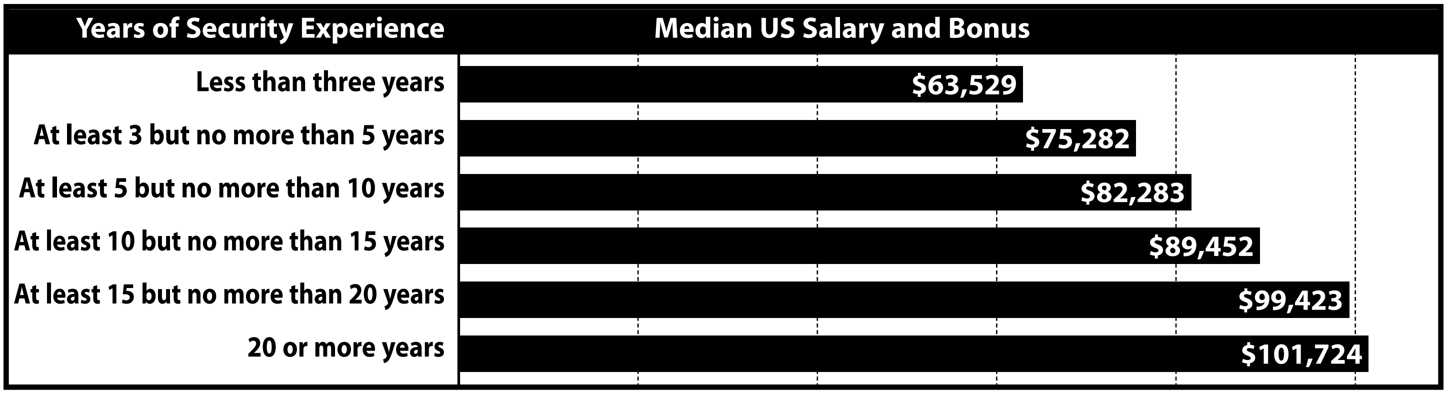
1. Compensation for information security jobs is strong and growing. The median income, including salary and bonus, for all US information security professionals is $81,558. Other nations pay less. The worldwide median is $77,050. Great Britain's median is $76,389 (94% of US). Canada's median is $67,982 (83% of US). The median for the rest of the world is $51,250 (63% of US).

Job Title	US Median Salary and Bonus	US Median Raise
Senior Security Executive with titles like Chief Information Security Officer, Chief Risk Officer, Chief Privacy officer, Chief Security Officer, Director of Security, Security Manager, and Other Senior Security Executive	$106,326	3.6%
Senior Technology Executive with titles like Chief Technology Officer, IT Director/ Manager, VP of Operations, Director of Operations, and Other Senior Technology Executive	$101,667	2.8%
Senior Technology and Policy Executive (combination of above two categories with strong emphasis on the technical)	$96,562	3.4%
Policy-Oriented Security Professional with titles like Information Security Officer, Security Analyst/Consultant (non-hands-on), Security Auditor (non-hands-on), Security Consultant, and Other Policy-Oriented Security Professional	$83,835	3.0%
Technical Security Professional with titles like Network Architect, Security Analyst/Consultant (hands-on), Security Auditor (hands-on), Security Engineer, Systems Engineer, Systems Integrator, Security Penetration Tester, Network Administrator, Programmer, Systems Administrator, and Web Security Manager.	$75,275	2.9%
Security Technology and Policy Professional (combination of previous two categories with strong emphasis on the technical, hands-on responsibilities)	$78,583	3.1%

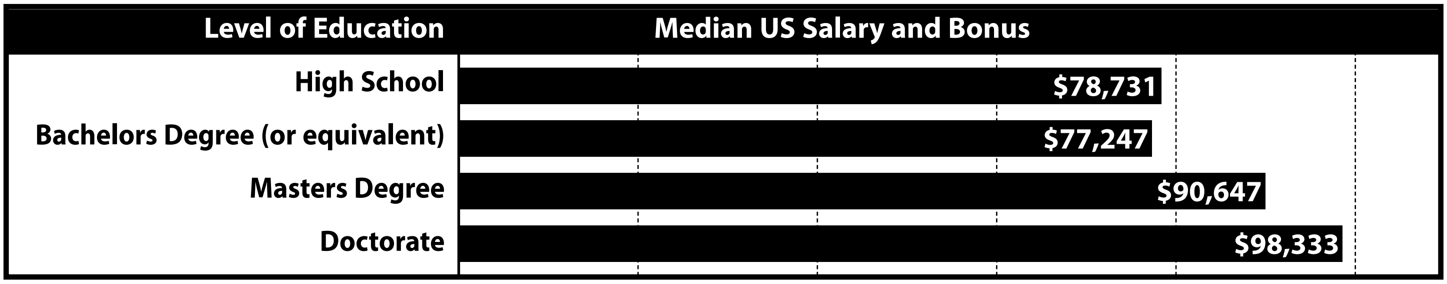
2. Larger employers pay more



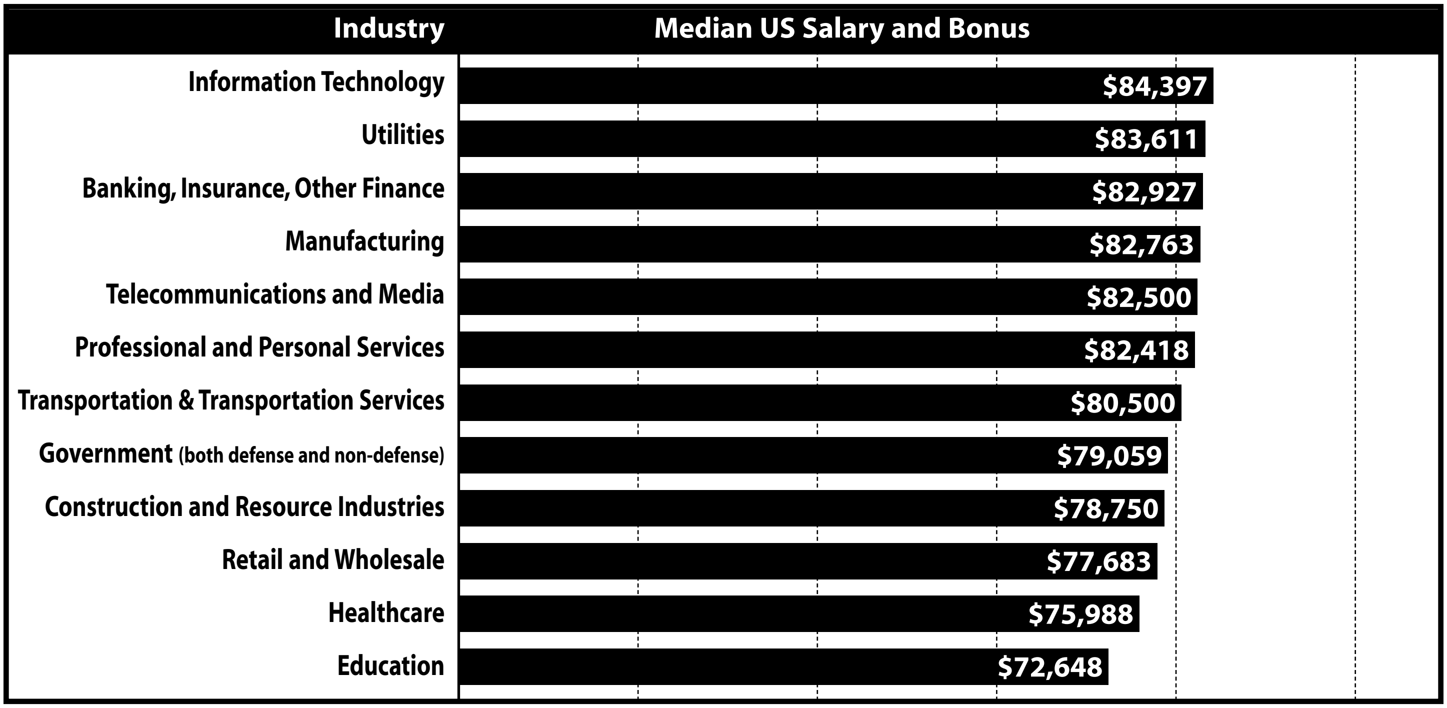
3. Years-of-experience in security closely correlates with level of compensation. Early in security careers, each year of experience accounts for about $4,000 of additional salary. Later each year accounts for approximately $2,000 of additional salary.



4. **Security professionals with bachelor's degrees do not earn more than people without college degrees. On the other hand, advanced degree holders get far more pay than people without masters or PhD degrees.**



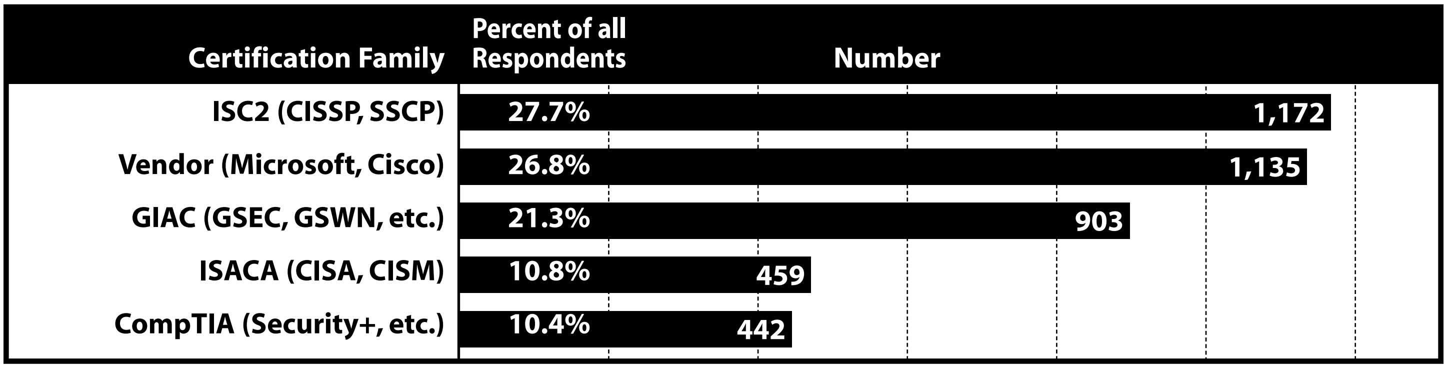
5. **The industry in which a security professional works affects his or her compensation. Information technology (including government security contractors), banking, manufacturing, telecommunications, and service industries pay more than other industries.**



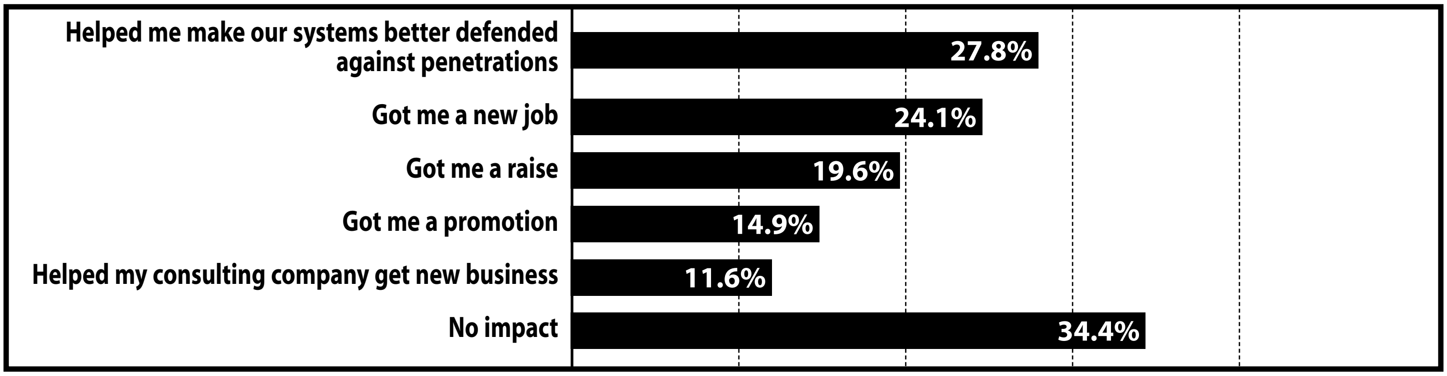
Professional certifications also impact compensation as the following section demonstrates.

Section II. The Value and Impact of Professional Certifications

6. **Most of the 4,278 people who completed the survey reported they hold at least one relevant professional certification. Some respondents hold multiple certifications.**

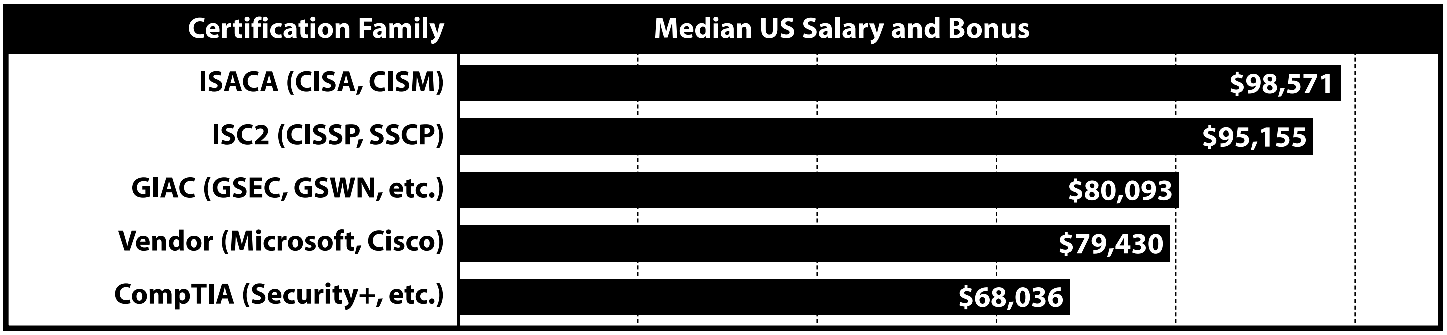


7. Certifications Matter. They matter most to individuals and consultants, but in about a quarter of the cases they actually help improve security too.

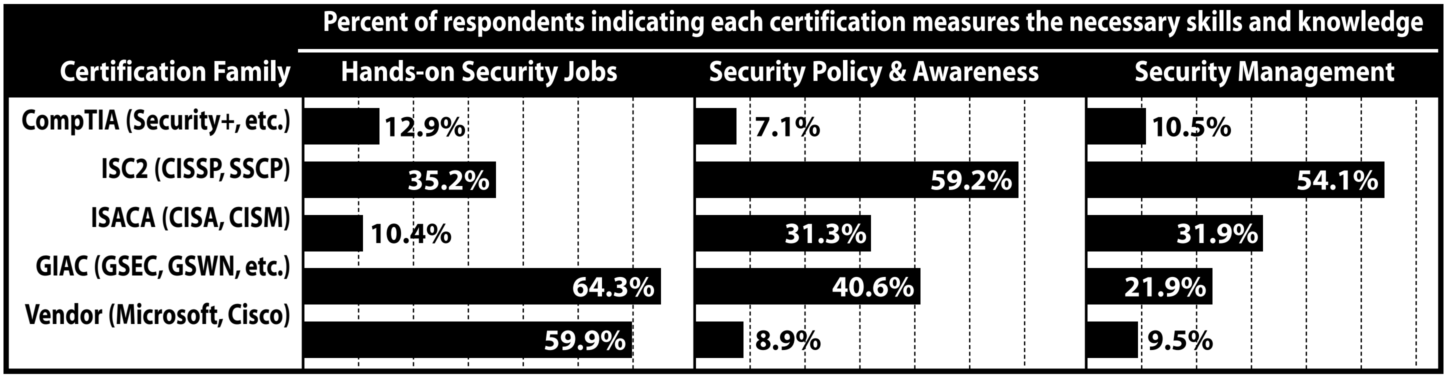


Percentages are of total respondents and total to more than 100% because more than one category could be chosen.

8. People who hold certifications from ISC2 and ISACA earn more than those who hold other certifications.



9. ISC2 certifications give an edge for management and policy jobs; GIAC certifications give an edge for hands-on security jobs.



Multiple votes were allowed.

10. Holders of CompTIA, ISC2, and ISACA certifications voted more than two-to-one that their certifications do not give them an edge for hands-on security jobs. They believe, overwhelmingly that GIAC certifications and software-specific security certifications were the certifications to use to ensure people with hands-on security jobs had the right skills.

	Which certifications measure the skills and knowledge for hands-on security jobs?				
Certification Held	**CompTIA**	**ISC2**	**ISACA**	**SANS GIAC**	**Software-Specific**
Non-software-specific certifications					
CompTIA	29%	39%	10%	63%	67%
ISC2	11%	35%	13%	76%	67%
ISACA	13%	46%	23%	72%	64%
Software- and tool-specific certification holders					
SANS	9%	25%	6%	90%	59%
Software-Specific	13%	34%	10%	69%	75%

Note that since they are able to vote for multiple certifications, the low votes for CompTIA and ISC2 and ISACA certifications are compelling proof that these certifications should not be relied upon for people with hands-on security responsibilities.

11. Confirming the data in the previous table, the non-tool-specific certifications (CompTIA, ISC2, and ISACA) had little or no impact on improving the security of systems to make them harder to penetrate. Only GIAC and the security certifications from system vendors led to specific system hardening improvements.

	Responses saying that the certifications led to improved system security		
Certifications held	**Listed specific hardening steps (44% of responses)**	**Listed no specific hardening steps (56% of responses)**	**Total (100% of responses)**
Software- and tool-specific certifications	**100%**	**89%**	**92%**
GIAC	85%	80%	78%
Commercial (Cisco, Microsoft, etc.)	15%	9%	13%
Non-software-specific certifications	**0%**	**11%**	**8%**
CompTIA	0%	7%	4%
ISC2	0%	5%	4%
ISACA	0%	0%	0%

12. Samples of hardening steps reported by the holders of security certifications:

1. I was able to harden the routers we have, develop a more formalized patch management strategy, and am now working on tightening up our identity management/provisioning policies. (GIAC GSEC)
2. Implemented back-ups, started monitoring logs for intrusion attempts, currently automating logging of internal machines and external intrusion attempts. Changed firewall to better system with syslog. (GIAC GSEC certification)
3. I have used these skills to better configure group policy, local firewalls, and even AD security resulting in hardened systems. (Microsoft MCSE Security Specialization)
4. Centralized OS patch management, centralized antivirus management, group policy templates from CISecurity.org (GIAC GSEC)

Section III. Factors That Delight and Frustrate Security Professionals

13. Respondents chose eight main themes in choosing "the single best thing your employer does to make you enjoy working." Unlike all the previous questions, the answers to this one were completely open-ended, offering no multiple-choice options. Nearly 3,000 people answered.

- (27.7%) **Trust:** that might include autonomy, freedom, respect, support, independence, apparent confidence, empowerment, and/or encouragement
- (11.6%) **Working hours and balance between work and other parts of life:** flexible hours, reasonable hours, and management understanding about hours
- (11.0%) **Compensation:** including good raises, and benefits, perks, bonuses
- (10.2%) **Training:** education, conferences, learning, tutorials, development, certifications. It's hard to imagine another field with members so thirsty for new technical knowledge
- (7.9%) **Challenge:** technical growth, and interesting work
- (5.9%) **Corporate culture:** environment, atmosphere, and "fun quotient"
- (5.6%) **Recognition:** including acknowledgment, praise, rewards, appreciation, and encouragement
- (5.0%) **Interesting projects,** including those chosen by the participants themselves and those that provided variety

14. Participants chose nine broad categories in defining "the single worst thing your employer does that makes working no fun at all." 2,804 responded.

- (20.2%) **Problems in management and leadership including lack of vision and micromanagement:** lack of planning, lack of understanding security's role, lack of technical ability, and/or lack of stability
- (9.9%) **Long/undesirable working hours,** including: long hours, undesirable hours, on-call requirements, heavy workload, understaffing, and overwork
- (8.4%) **Low compensation** (including raises)
- (7.7%) **Politics** and too-frequent reorganizations
- (6.4%) **Funding,** budget issues, lack of "investment," and lack of resources
- (6.3%) **Lack of authority,** had no influence, garnered no attention from management, and/or felt no confidence from management
- (6.0%) **Bureaucracy and red tape** including paperwork, trouble tickets, and time-tracking
- (5.7%) **Poor communications,** including lack of direction
- (3.7%) **Lack of training**

Section IV. Critical Skills Necessary for Advancement *(Updated July 10, 2007)*

15. Presentation and writing skills are (slightly) more important even than technical knowledge for career advancement. Critical thinking and judgment, teamwork, ability to lead change, and knowledge of the business followed closely in importance. SANS Technology Institute's new masters' degree programs in information security engineering and in information security management are different from other masters' degree programs because of the leadership focus; SANS programs ensure that the graduates master speaking, writing, and teaching, as well as ensuring that they have the best technical education available (www.sans.edu).

Area	Very important	Important	Not important	No opinion
Writing ability (incl documentation)	69%	28%	0%	1%
Verbal communication ability	68%	29%	0%	1%
Technical knowledge	66%	31%	2%	1%
Critical thinking and judgment	69%	26%	2%	3%
Teamwork and collaboration	52%	42%	3%	3%
Ability to lead change	52%	39%	5%	4%
Business knowledge/acumen	40%	50%	6%	3%
Cross-functional influence	35%	50%	7%	9%
Influence	33%	52%	8%	7%
Facilitation	24%	56%	11%	10%
Mentoring and coaching	19%	57%	17%	7%
Strategic business planning	22%	48%	21%	10%

SANS Institute
8120 Woodmont Ave. #205
Bethesda, MD 20814
1-301-951-0102
www.sans.org