Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cybersecurity Professional Trends: A SANS Survey

Copyright SANS Institute
Author Retains Full Rights
Cybersecurity Professional Trends: A SANS Survey

A SANS Analyst Survey
A Joint Project of SANS GIAC and the SANS Analyst Program
Advisors: John Pescatore, Barb Filkins, Tracy Lenzner and SANS GIAC
May 2014

Sponsored by
Arbor Networks
Holding one or more certifications in information security is the leading factor to successful careers, based on results of the SANS survey on salaries and certifications taken by more than 4,000 respondents in February and March 2014.

This survey follows the SANS 2008 Salary and Certification Survey,¹ which predicted IT security salaries to rise and certifications to become increasingly important as new technologies—and methods of exploiting them—evolve.

Over the past six years, salaries have not risen quite as predicted. In 2008, the largest group of respondents selected the $80,000–$99,999 pay range, which was also the single largest category selected in our current survey. This pay range should be higher, given the tough nature of the jobs IT security professionals shoulder—and the specialized skills and business acumen required in such positions. Fortunately, a larger group of respondents—49% in 2014 as opposed to 38% in 2008—are earning $100,000 or more a year, indicating that salaries are rising for managers.

Many variables contribute to salaries, including years of experience, industry, education and—especially—certifications. In 2008, the majority of hiring managers felt that certifications were an important (or key) requirement for hiring. The 2014 results support this finding, but from the standpoint of those obtaining certification. In this year’s survey, 58% believe that holding one or more certifications is critical to their career success.

Following certifications, respondents to this year’s survey cite continued education and networking as critical to career success. Interestingly, respondents ranked bachelor’s and master’s degrees lower than expected as contributors to career success. Perhaps this is because higher education is now the norm (76% hold a bachelor’s degree or higher) and the need for specialized skills such as incident handling and response, audit and compliance, and firewall/IDS/IPS/SIEM skills has risen. The majority of those who took this year’s survey (72%) represented non-management positions, and 33% want to move into management and leadership over the next five years. However, moving from administrative titles to management titles will take growth in peer networking, technical and executive skills, and education, ultimately requiring more of these respondents to return to the classroom to pursue the highly coveted MBA or other advanced degree programs.

In both our 2014 and 2008 surveys, banking, finance and insurance as a combined group represented 18% of respondents. The next three segments—information technology/management, government (defense) and government (nondefense)—each accounted for 11%. Consulting and professional services, together, accounted for 10%. The distribution of industries represented is shown in Figure 1.

The top vertical industries represented here coincide with those with the highest-value sensitive information targeted by attackers: financial records and national security information. IT/management, consulting and professional services can also include government contractors, law firms and others with sensitive clientele to protect, indicating that organizations providing services to these verticals could provide new areas of career growth for IT security professionals.
Organization Size

The 2008 survey concentrated on the demographics for a workforce located predominantly in the United States. Today, the global nature of organizations being supported and their size both impact the IT security professional’s job functions and salary. Twenty-six percent of respondents indicated they worked for companies with 15,000 or more employees, which were predominately global companies.

The distribution of organization sizes and global versus domestic businesses is shown in Figure 2.

Based on the global nature of the security industry and the challenges and opportunities it brings, those seeking employment would be well served by taking a broader view with respect to job locations. There are both opportunities and rewards beyond the borders of the United States.

Remaining within the United States for employment may mean working at a smaller organization. It's commonly known that the smaller the company, the smaller the IT staff to support it. Depending on an individual’s career goals, employment at a small company can enable the person to gain broader experience managing more with fewer resources. In the larger organizations, more specialized skillsets and certifications are considered valuable, which we will discuss later in this paper.

Figure 2. Size of Respondent Organizations
Job Titles

Most people closely link information technology and security, especially in the area of infrastructure, typically defined as systems, servers and networks. Although there are probably hundreds of titles in the IT security workforce, this survey concentrated on 19 specific titles and provided the catchall category of “Other.”

In 2008, the security engineer or architect was the most popular job title (slightly greater than 12%) followed closely by information security analyst (slightly less than 12%). In our current survey, both titles have grown. The title of security analyst takes the lead at 23%, followed by security engineer or architect at 15%. Management-oriented job titles occupy third and fourth places, as shown in Figure 3.

The “Other” category also included a number of variations of information security manager, some in the area of continuity, information assurance, SOC management and audit. Some new Internet of Things job titles were also represented under the “Other” category, including industrial control systems specialist and instrumentation and control engineer.
Overall, when sorted by their title, 72% of respondents hold non-management titles and 28% have a managerial title (see Figure 4).

Education

Formal education continues to be an important consideration for our respondents. As shown in Figure 5, slightly more than 75% of all respondents have at least a bachelor’s degree (or equivalent), with 30% having a master’s degree, MBA, or higher. The Burning Glass Technologies’ Report on the Growth of Cybersecurity Jobs is consistent with these findings, stating that over 84% of cybersecurity job postings require applicants to hold at least a bachelor’s degree.²
Experience

The same Burning Glass report\(^3\) also identifies that four years of experience are required for two-thirds of cybersecurity job postings. In our survey 83% of survey respondents had four or more years of experience, as illustrated in Figure 6.

It is also interesting to note, however, that the majority (60%) of our respondents has 10 years or less of experience, an indication that new talent continues to be attracted to the field. Both government and private industries are contributing to building the future workforce with awareness campaigns on the careers available and skills needed, as well as scholarships and opportunities to test for aptitude.

---

IT security is one of the fastest growing careers, and the outlook for the future is bright. Overall, professionals involved with information security command salaries and bonuses that are well above the national average for US workers. In our survey 49% of respondents make $100,000 or more—mostly attributed to those with management roles, while the largest single group (23%) selected the $80,000–$99,999 range, representing those with administrator or engineering roles.

Figure 7 shows the overall distribution of income ranges, including salary and bonuses.

For all subsequent analysis, SANS excluded any incomes reported by respondents that were higher than $250,000 per year from our calculation of average salaries. Given this, when grouped together, respondents earned on average slightly more than $102,000 ($102,505) annually, with a significant difference between the overall average for the management ($121,376) and non-management ($95,149) categories.

Figure 7. Respondents’ Income Range in US Dollars

---

4 [www.bls.gov/emp/ep_table_103.htm](http://www.bls.gov/emp/ep_table_103.htm)
Experience: A Key Factor

As one would expect, cybersecurity salaries climb based on years of experience. The average professional starts out at nearly $74,000 a year, based on responses, while those with 20 years of experience earn more than $123,000 a year. That’s a differential of almost $50,000 in yearly wages developed over 20 years of experience. Incrementally that would represent raises of about $2,500 for each year of experience.

Table 1 provides the overall average salaries by respondent category and years of experience.

<table>
<thead>
<tr>
<th>Years of Experience</th>
<th>Average Across Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–3</td>
<td>$73,697</td>
</tr>
<tr>
<td>4–6</td>
<td>$88,778</td>
</tr>
<tr>
<td>7–10</td>
<td>$103,523</td>
</tr>
<tr>
<td>11–15</td>
<td>$117,056</td>
</tr>
<tr>
<td>16–20</td>
<td>$123,556</td>
</tr>
<tr>
<td>20+</td>
<td>$123,399</td>
</tr>
<tr>
<td>Overall</td>
<td>$102,505</td>
</tr>
</tbody>
</table>

Both management and non-management positions show progressive salary increases with years of experience, all the while management income remains on average 22% higher than non-management income, regardless of the years of experience.

Figure 8 shows the distribution of income ranges based on years of experience and whether the respondent would be considered management or non-management.
**Titles Matter**

Titles also impact compensation packages. As shown in Table 2, management titles are earning the most; however, these numbers seem low to SANS, given the responsibilities and liabilities a typical CISO/CSO experiences. We would expect, for example, that these roles would average closer to $200,000 a year for a person with 15 years of experience.

![Table 2. Average Income by Title and Years of Experience (Top 10 Job Titles)](image)
Education and Experience Matter

Education also impacts compensation packages, as shown by our data. Respondents holding bachelor’s degrees and 7 to 10 years of experience command average incomes in excess of $100,000 annually. Those with more advanced degrees achieve this level of pay sooner.

Table 3 shows the average salary by education and years of experience for survey respondents.

<table>
<thead>
<tr>
<th>Education</th>
<th>0–3 yrs</th>
<th>4–6 yrs</th>
<th>7–10 yrs</th>
<th>11–15 yrs</th>
<th>16–20 yrs</th>
<th>+20 yrs</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>High school diploma</td>
<td>$47,917</td>
<td>$75,938</td>
<td>$115,000</td>
<td>$88,235</td>
<td>$102,222</td>
<td>$123,333</td>
<td>$89,013</td>
</tr>
<tr>
<td>Some college or technical School</td>
<td>$66,761</td>
<td>$86,560</td>
<td>$100,726</td>
<td>$115,682</td>
<td>$116,438</td>
<td>$117,073</td>
<td>$101,014</td>
</tr>
<tr>
<td>Associate’s (2-year) degree</td>
<td>$62,302</td>
<td>$85,000</td>
<td>$93,418</td>
<td>$107,569</td>
<td>$101,528</td>
<td>$106,667</td>
<td>$90,601</td>
</tr>
<tr>
<td>Bachelor’s (4-year) degree</td>
<td>$71,564</td>
<td>$84,619</td>
<td>$100,862</td>
<td>$115,782</td>
<td>$123,561</td>
<td>$127,733</td>
<td>$98,510</td>
</tr>
<tr>
<td>Some graduate studies</td>
<td>$79,479</td>
<td>$87,069</td>
<td>$100,952</td>
<td>$122,842</td>
<td>$127,500</td>
<td>$127,667</td>
<td>$106,439</td>
</tr>
<tr>
<td>Master’s degree or MBA</td>
<td>$82,906</td>
<td>$97,109</td>
<td>$109,319</td>
<td>$120,964</td>
<td>$132,816</td>
<td>$125,464</td>
<td>$109,705</td>
</tr>
<tr>
<td>PhD, JD, or equivalent</td>
<td>$121,667</td>
<td>$114,231</td>
<td>$128,462</td>
<td>$119,600</td>
<td>$150,000</td>
<td>$116,250</td>
<td>$125,244</td>
</tr>
</tbody>
</table>

The 2008 and 2014 surveys used slightly different categories of experience. For example, the 2008 survey lumped up to four years of experience together, whereas the 2014 survey makes analyses based on up to three years of experience being lumped together. Salaries for respondents with fewer than three years of experience remain consistent with what was reported in the 2008 survey for respondents with fewer than four years of experience. An employee with an associate’s degree in 2008 netted an average salary of $59,503, as compared with $62,302 in 2014. A bachelor’s degree in 2008 with same experience earned $74,807, as compared with $71,564 reported in this survey. The additional year of experience contained in the 2008 survey may explain the small difference in salary associated with the bachelor’s degree.

There is a significant increase in salaries for those who have been in the industry for more than 10 years and hold more advanced degrees. Just over one-quarter (28%) of respondents hold a master’s degree, and 2% reported holding a PhD, JD, or equivalent. As the digital threat continues to advance—and security and privacy become part of our functionality in technology, products and services—the need for advanced degrees is predicted to continue to be in high demand.
The Top 10: Income by Industry and Experience

Experienced IT security professionals working in the manufacturing industry and consulting services have much more earning power than those in education, an industry notorious for strapped resources. Table 4 presents average income by industry and years of experience, ordered by average salary, for the 10 most prevalent industries as represented in this survey.

<table>
<thead>
<tr>
<th>Industry</th>
<th>0–3 yrs</th>
<th>4–6 yrs</th>
<th>7–10 yrs</th>
<th>11–15 yrs</th>
<th>16–20 yrs</th>
<th>+20 yrs</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>$82,619</td>
<td>$112,714</td>
<td>$105,000</td>
<td>$116,250</td>
<td>$125,625</td>
<td>$135,667</td>
<td>$111,585</td>
</tr>
<tr>
<td>Consulting/Professional Services</td>
<td>$75,750</td>
<td>$84,133</td>
<td>$114,753</td>
<td>$132,476</td>
<td>$121,216</td>
<td>$127,674</td>
<td>$109,699</td>
</tr>
<tr>
<td>Energy/Oil and Gas/Utilities</td>
<td>$87,188</td>
<td>$96,125</td>
<td>$116,273</td>
<td>$121,100</td>
<td>$118,182</td>
<td>$126,250</td>
<td>$108,658</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>$77,500</td>
<td>$88,654</td>
<td>$104,697</td>
<td>$117,872</td>
<td>$116,071</td>
<td>$120,000</td>
<td>$105,151</td>
</tr>
<tr>
<td>Information Technology/Management</td>
<td>$73,108</td>
<td>$84,821</td>
<td>$105,517</td>
<td>$126,619</td>
<td>$130,833</td>
<td>$128,261</td>
<td>$105,111</td>
</tr>
<tr>
<td>Government (Defense)</td>
<td>$75,244</td>
<td>$90,390</td>
<td>$100,285</td>
<td>$109,762</td>
<td>$125,778</td>
<td>$126,310</td>
<td>$103,626</td>
</tr>
<tr>
<td>Banking/Finance/Insurance</td>
<td>$73,500</td>
<td>$87,566</td>
<td>$105,815</td>
<td>$116,900</td>
<td>$131,508</td>
<td>$129,643</td>
<td>$103,050</td>
</tr>
<tr>
<td>Health Care</td>
<td>$67,976</td>
<td>$91,083</td>
<td>$95,446</td>
<td>$115,847</td>
<td>$116,500</td>
<td>$123,810</td>
<td>$98,566</td>
</tr>
<tr>
<td>Government (Nondefense)</td>
<td>$78,182</td>
<td>$88,301</td>
<td>$95,176</td>
<td>$108,021</td>
<td>$118,636</td>
<td>$109,886</td>
<td>$98,150</td>
</tr>
<tr>
<td>Education</td>
<td>$65,357</td>
<td>$74,811</td>
<td>$80,167</td>
<td>$102,619</td>
<td>$108,148</td>
<td>$103,250</td>
<td>$85,609</td>
</tr>
</tbody>
</table>
Certification for Career Success

Survey respondents report that security certifications are critical to their success. Reasons for seeking certifications range from having a personal motivation to improve skills to gaining a competitive advantage in securing jobs or contracts.

Employers often use certifications as a requirement for employment and as a way to differentiate candidates during the interview process. Certifications are also considered in pay increases and employee advancements. Earning a certification builds skillsets, demonstrates a level of competence in the subject matter and demonstrates, by the investment of time to learn new skills, that the certification holder is dedicated to his or her career.

Certifications are more frequently required in IT security than in other, more general IT roles, according to the latest Burning Glass report.\(^5\) For example, many government positions require cybersecurity workers to hold a certification as part of the Department of Defense (DoD) 8570 directive.\(^6\)

Industry-led certifications provide a benchmark for skills delivered through training and accreditation. They offer metrics that the training is aligned with tangible skills and knowledge required. Figure 9 reveals that 58% of respondents believe security certifications are the biggest contributors to their career success.


\(^6\) http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html
Write-in answers about the value of certifications included strong statements including the need for certification just to be employed. Currently, a wide range of certifications, training and education programs are available, particularly as both the private and public sectors ramp up cyberworkforce initiatives. IT security professionals, at any level, who are interested in career growth and advancement can acquire new skills and knowledge through the certification process.

**Sharing the Costs of Certification**

Employers also recognize the value of certification for cybersecurity professionals. Almost 80% of respondents reported their employers either completely pay for (65%) or share the cost of (15%) obtaining certifications with the employee. Only 16% stated that they pay for the certification themselves, as illustrated in Figure 10.

![Pie chart showing who generally pays for certifications](image)

*Figure 10. Who pays for certification?*
Value of Certification

Certifications make a difference in compensation. The survey asked respondents what they believed the salary differential for the various certifications to be. Respondents varied significantly on their responses; however, it appears that increases of up to 5% of salary accompany many certifications.

Based on survey responses, the perceived value of the top certifications fell into what we consider to be four value tiers, as shown in Table 6.

<table>
<thead>
<tr>
<th>Value Tier</th>
<th>Certification</th>
</tr>
</thead>
</table>
| First      | GIAC Security Expert (GSE)  
.ISC(2) Certified Information Systems Security Professional (CISSP) |
| Second     | GIAC Certified Forensics Analyst (GCFA)  
.GIAC Penetration Tester (GPEN)  
.GIAC Industrial Cyber Security Professional (GICSP) |
| Third      | GIAC Certified Incident Handler (GCIH)  
.ISACA Certified Information Systems Auditor (CISA)  
.GIAC Security Essentials Certification (GSEC)  
.GIAC Certified Intrusion Analyst (GCIA)  
.GIAC Security Leadership Certification (GSLC) |
| Fourth     | CompTIA Security+  
.ISC(2) Certified Cyber Forensics Professional (CCFP)  
.EC-Council Certified Ethical Hacker (CEH)  
.Cisco Certified Network Professional (CCNP)  
.Cisco Certified Security Professional (CCSP) |

When it comes to making a difference in earning potential, five GIAC certifications (GSEC, GCIH, GCIA, GPEN and GCFA) were included in the Top 10 list of recognized information security certifications for making an impact in compensation levels for security professionals. Given the popularity of certification to career success, the investment involved and the potential for increased earning power, this is clearly an area to explore in future surveys, gaining insight from those who have more information on the actual salary implications of certifications.
We asked survey respondents to address four key areas of change that represent key trends within the security industry:

- What is the focus of the individual information security professional today, and how will it change in the next five years?
- What skills are in demand by the industry, and how will this change over the next two years?
- How stable is employment in the industry in the minds of its workforce?
- What are the factors in attracting and retaining employees with key security skills and experience?

**Changing Focus to Advance**

The three primary areas of focus selected by information security professionals include management/leadership (selected by 25% of respondents), administration (selected by 18%) and engineering (also 18%). This aligns with the roles respondents reported at the beginning of the survey. Figure 11 shows the focus of survey respondents.
Information security is a broad field. A key benefit is the opportunity it offers to learn new skills and focus on new technologies or domains. IT security professionals can quickly become extinct if they don’t continually update their skills as new technologies emerge. The ability to continually identify, adapt and update critical skills and potential gaps in experience and training will be key to professional survival and success. In our survey 67% of respondents reported changing focus at least one to three times during their careers, and 19% have changed focus four to six times, as shown in Figure 12.

Crossover into security from operational positions was represented in the changes in focus, according to the open-ended responses to this question. The change of focus specifically involved moving from IT to security. In addition, several respondents entered the security field from unique perspectives—speechwriter, welding inspector or computational linguistics. One respondent summed up the potentially dynamic nature of this field and its impact on career focus saying, “We tend to change focus multiple times a day to tackle whatever the most pressing issue is.”
Jobs, Skills, Staffing and Incentives (CONTINUED)

Figure 13 shows what respondents anticipate their focus will be in the next five years.

**What do you anticipate your focus will be for the next five years?**

![Figure 13. Areas of Focus for Security Professionals Next Five Years](image)

From these results, it appears that 33% are moving toward management/leadership in the next five years. However, 25% of these respondents are already in management and are simply changing their focus within that category. That means another 8% of survey takers are moving toward management, while 16% anticipate no change and 10% are unsure of where they are headed.

Table 7 compares those who actually stated their planned change in focus against their focus today.

<table>
<thead>
<tr>
<th>Area of Focus</th>
<th>Today</th>
<th>Next 5 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management/Leadership</td>
<td>25.4%</td>
<td>33.1%</td>
</tr>
<tr>
<td>Administration</td>
<td>18.0%</td>
<td>5.2%</td>
</tr>
<tr>
<td>Engineering</td>
<td>17.8%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Other</td>
<td>11.9%</td>
<td>4.3%</td>
</tr>
<tr>
<td>Audit</td>
<td>10.7%</td>
<td>5.9%</td>
</tr>
<tr>
<td>Forensics</td>
<td>7.7%</td>
<td>9.7%</td>
</tr>
<tr>
<td>Testing</td>
<td>4.4%</td>
<td>3.3%</td>
</tr>
<tr>
<td>Development</td>
<td>4.1%</td>
<td>3.0%</td>
</tr>
</tbody>
</table>
Many of those newly moving into management appear to be coming from the administration ranks, the category that shows the biggest difference between current and future career paths. Some may also move into forensics, which shows a slight growth. Under the “Other” comments, respondents wrote in roles that were not on the list that they see themselves filling in next five years. Some of the top roles include:

- Compliance
- Teaching or education
- Incident handling, forensics and malware analysis
- Research
- Supply chain cybersecurity
- Cloud and mobility administration
- Industrial control systems or utilities security management
- Retirement

Other job positions, including engineering and audit, are also on the decline in terms of where people see themselves in five years. This trend indicates a significant gap in technical roles if educators and mentors don’t keep producing new administrative technical staff to fill the gap.
Incident handling and response is a key skill for managers and non-managers both today and in the future. Other key non-management skills include audit and compliance, managerial or leadership skills, firewall/IDS/IPS/SIEM management, and analytics and intelligence. Additional managerial skills in demand include cloud computing/virtualization, analytics and intelligence, and audit and compliance.

Incident response was one of the top write-in answers in response to where respondents see themselves in the next five years. This is consistent with most sought-after skills for non-managers, which include incident handling and response (35%), audit and compliance (32%), and advanced firewall and IDS management skills (30% each).

The top skills in demand for management level staff also include incident handling and response (15%) and audit and compliance (13%). This is followed by managerial/leadership (13%), then firewall/IDS/IPS skills, SIEM management, and analytics and intelligence (about 11% each).
The skills outlook changes slightly for both categories when participants were asked to identify what skills would be in demand over the next two years. Understanding the technical and nontechnical issues in law, financial markets, psychology, human factors, user interface, adoption and other areas will be required as security evolves from silos to a multidisciplinary field. Figure 15 illustrates the skills participants believe will be in demand.

Figure 15. Skills in Demand for Security Professionals for the Next Two Years
For non-managers, incident handling and response (31%) will still remain the number one skillset, followed by cloud computing/virtualization (29%), analytics and intelligence (26%), audit and compliance (24%) and intrusion detection (24%). Managers will see similar trends with cloud computing/virtualization (13%), incident handling and response (12%), analytics and intelligence (11%) and audit and compliance (10%) being the most sought-after skills.

In summary, incident response and handling is the skill most in demand today for both management and non-management security professionals alike. This trend will continue through 2016, but will be complemented by the necessary growth in skills in cloud computing and “big data”—specifically analytics and intelligence, audit and compliance, and the increased need to protect sensitive data being accessed through new cybervectors.

As organizations respond to increasing numbers of complex attacks and expanded threat landscapes, they must seek security professionals with technical, hands-on experience in a variety of new, rapidly evolving technologies, such as advanced malware protection, threat detection, intelligence and analytics, continuous monitoring, security architecture and data-oriented platforms.

For those working in a global environment, it is likely that emphasis will also be placed on key skills in international privacy, compliance, technology law and risk frameworks, both for business and government.

**Soft Skills in High Demand**

Employers don’t just seek specific technical skills when they are hiring—they look at the whole person. For those working to improve their careers or keep the jobs they love, soft skills are critical. Some are essential, and some are geared toward management.

**Essential soft skills:**
- Broad and deep technical expertise
- Program delivery
- Enterprise experience
- Progressive track record
- Credentials (education, training, certifications, licenses, clearance, awards/recognition)
- Value and ROI

**Soft skills for the upwardly mobile employees:**
- Leadership (credibility, trust, responsiveness, respect, ethics, business acumen)
- Communication skills (writing, speaking, presenting, ability to achieve stakeholder engagement and adoption)
- Interpersonal skills (street smarts, diplomacy, confidence, flexibility, sense of humor, professionalism, polish, grooming)
- Industry contribution or involvement (private/public partnerships, media, alliances, forums, internships, advisory boards)
Staffing by Industry

According to a BankInfoSecurity blog,7 the cybersecurity job market is strong, and unemployment in this sector remains low.

Survey respondents appear to agree. According to responses, the past 12 months have been strong for IT security careers. During that time, 43% of respondent organizations increased staff, with 17% of them increasing staff by more than 10%. A small number of respondents did report reductions, but this was not the norm (see Figure 16).

Open-ended comments left by respondents shed some light on why many organizations report no change in their staffing over the next 12 months. Acquisitions/mergers, lack of qualified candidates and current employees increasing their workload are all main reasons noted for keeping the staff count at a constant level.

---

A recent article about the Top 10 Silicon Valley tech job trends on InfoWorld.com states a tech hiring boom is under way, as more than 88% of CIOs in the Northern California Bay area are looking to expand or fill vacant positions. Projections for the next 12 months corroborate this rosy outlook, as shown in Figure 17.

More than one-third of respondents (35%) expect their organization to increase its cybersecurity staff—12% expect a staff increase of more than 10%, while fewer than 5% of respondents expect a reduction of cybersecurity staff. This is good news for IT security professionals looking to advance their careers or change to hotter focus areas, particularly if those professionals are up to date with the security technologies and certifications needed.

---

Percentage of respondents expecting their organizations to increase cybersecurity staff

![Bar chart showing projected staffing changes for the next 12 months.](image)

**Figure 17. Projected Staffing Changes for the Next 12 Months**

---

Incentives

In a strong job market, such as the one IT security professionals are experiencing today, incentives can mean the difference between retaining, advancing or hiring the employee of your choice or losing them to another employer.

If employers are not providing the right incentives, they could inadvertently be creating an environment of dis-incentives that would make employees seek changes in employment status. Lack of advancement, stagnant wages, inadequate benefits and lack of job stability are the primary reasons for seeking an employment change, according to respondents. Figure 18 shows the factors that respondents felt were important in prompting change in current employment status.

![Figure 18. Important Factors Prompting Changes in Employment Status](chart.png)

Lack of advancement, stagnant wages, inadequate benefits and lack of job stability are the primary reasons for seeking an employment change.
Just 6% stated that they were not seeking a change in employment. Echoing the positive nature of staffing trends, only 3% had concerns over being laid off, and fewer than 1% had actually been laid off.

Surprisingly, while lack of advancement and seeking better salary and benefits are cited as factors for job change, these are not necessarily incentives for individuals to stay with their current employer. Variables that incentivize people to stay with employers are less tangible and include personal satisfaction, continued growth opportunities and a challenging work environment. Figure 19 shows what incentivizes respondents, as employees, to stay with their employers.

More than 70% of respondents indicated that personal job satisfaction was the top reason they stay in their current position, as opposed to the 66% who cite salary/compensation and 62% who cite continued growth opportunities as incentives to remain with their current organizations. Non-managers are more incentivized by continuing education opportunities, benefits and bonuses than managers.

Open-ended comments by respondents indicate many are seeking better lifestyle options such as flexible hours, relocation and a better work/life balance, as well as the ability to keep their technical skills sharp and participate in a more hands-on environment.
Based on the results of the survey, the GIAC and SANS Analyst teams asked a human resources professional for guidance on what these results mean for IT security professionals moving forward.

Long-term career success means being able to self-manage. Take these actions to guide your career steps:

1. Define your path and make a plan.
2. Set goals, timelines and deliverables to ensure focus on your plan.
3. Assess progress and embrace peer assessments.
4. Conduct a gap analysis and fill in any gaps with training, certifications and education.
5. Continuously monitor progress based on individual metrics for success.

Keep in mind, though, career success is relative. Earning power, opportunity and career trajectory vary significantly. External factors such as organization, industry sector, organizational size, location, market conditions and senior leadership are not generally in one’s control.

With that said, anyone wanting to move up the food chain into management or desiring job stability will continuously need to shore up their career portfolios. Peer networking, technical and executive skills, advanced training and education are key to IT security professionals, regardless of their level and/or experience.
The SANS 2008 Salary and Certification Survey concluded with the statement that, “despite the current economy, the demand for qualified security professionals is predicted to increase through 2016, according to the Bureau of Labor Statistics.” Six years later, the 2014 SANS Salary Survey reinforces this prediction.

As the fight against online crime and cyberwarfare continues to escalate, so will the demand for highly trained cybersecurity professionals with relevant skills. This global war means opportunity at every level for IT security professionals over the next decade. Cybersecurity professionals will be able to command high salaries, earn excellent incentives, experience job and career satisfaction and gain opportunities to build skills and knowledge.

The opportunity is there for IT and security professionals to become their own career ambassadors through continuous professional development, relevant/advanced technical expertise, business leadership, organizational and industry contributions, and efforts to stay ahead of industry trends.

SANS would like to thank this paper’s sponsor:
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>Online TXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>