Ponemon INSTITUTE

Understaffed and at Risk:
Today's IT Security Department

Sponsored by HP Enterprise Security

Independently conducted by Ponemon Institute LLC

Publication Date: February 2014

Understaffed and at Risk: Today's IT Security Department

January 2014

Part 1. Introduction

One of the biggest barriers to a strong security posture, according to Ponemon Institute research, is having a team of security professionals that can deal with complex and serious internal and external threats to the organization. *Understaffed and at Risk: Today's IT Security Department* was conducted by Ponemon Institute and sponsored by HP Enterprise Security to understand how effective organizations are in hiring and keeping enough skilled and expert staff to meet their IT security mission.

The study focuses on how organizations are attracting and retaining qualified IT security professionals. Topics included:

- How the demand for skilled IT security personnel has changed since 2012.
- The number of jobs that go unfilled because of difficulties in finding qualified personnel.
- The length of time spent on the job and the problem of high turnover, especially among the more senior security practitioners.
- Compensation packages that might not be adequate to attract and keep staff.
- The most desirable skills and backgrounds for security staff.

We surveyed 504 human resources and IT security specialists in the United States. To ensure a knowledgeable respondent, we only permitted individuals to complete the survey who are responsible for attracting, hiring, promoting and retaining IT security personnel within their organizations.

Some key findings from this research include:

- The IT security function is understaffed. Seventy-percent of respondents say their organizations do not have enough IT security staff.

- The average headcount of an IT security function is expected to grow from 22 staff members in 2013 to 29 in 2014.

- On average, 58 percent of senior staff positions in IT security went unfilled in 2013. Respondents are somewhat optimistic that the hiring of senior IT security personnel will improve and the percentage of unfilled positions is expected to decrease to 49 percent in 2014.

- On average, 36 percent of staff positions went unfilled in 2013. In contrast to filling senior-level positions, the percentage of unfilled staff positions is expected to increase to 40 percent in 2014.

- Senior security executives don't stay in their jobs very long. On average, CISOs and others in a similar position leave after 2.5 years. Those in a technician or comparable role stay an average of 4 years.

- Decisions about IT security staffing and recruitment are most likely made by human resources and corporate IT.

- On-the-job experience and professional certifications make the biggest difference when hiring a security practitioner. Most job recruiting takes place at conferences.

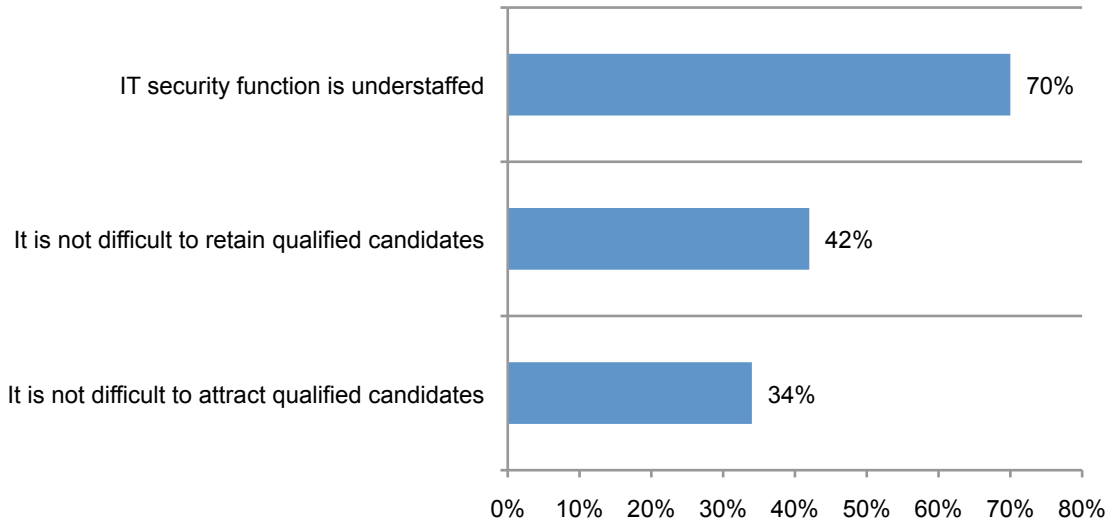
- By far, salary is the most important part of a hiring package. Key to stopping turnover is the ability to offer a competitive salary.

Part 2. Key Findings

Following is a summary of the key findings. The complete audited findings are presented in the appendix of this report.

Most organizations in this study do not have the depth and breadth of qualified security professionals. According to Figure 1, the majority of respondents (70 percent) say their organization's IT security function is understaffed. Only 34 percent say they have no difficulty in attracting qualified candidates and 42 percent say they have no difficulty in retaining these experts.

Figure 1. Challenges to staffing the IT security function
Strongly agree and agree response combined



Trends in hiring indicate a steady growth in headcount. Figure 2 shows interesting trends in staffing. According to respondents, the total headcount is growing. On average, the headcount for organizations represented in this study grew from 18 in 2012 to 22 this year. In 2014, the average is expected to grow to 29.

Figure 2. Average number of staff in IT security departments

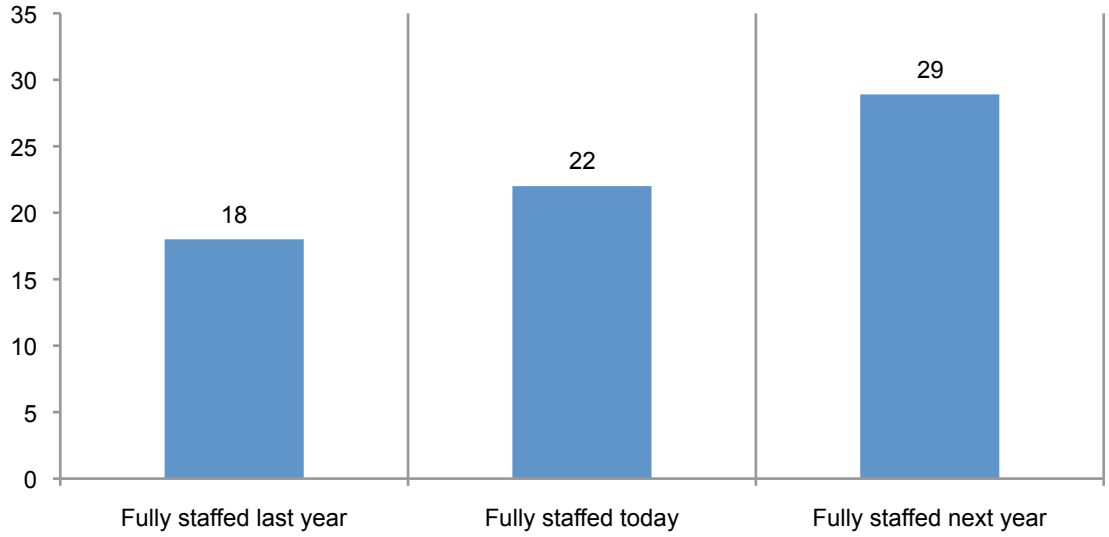
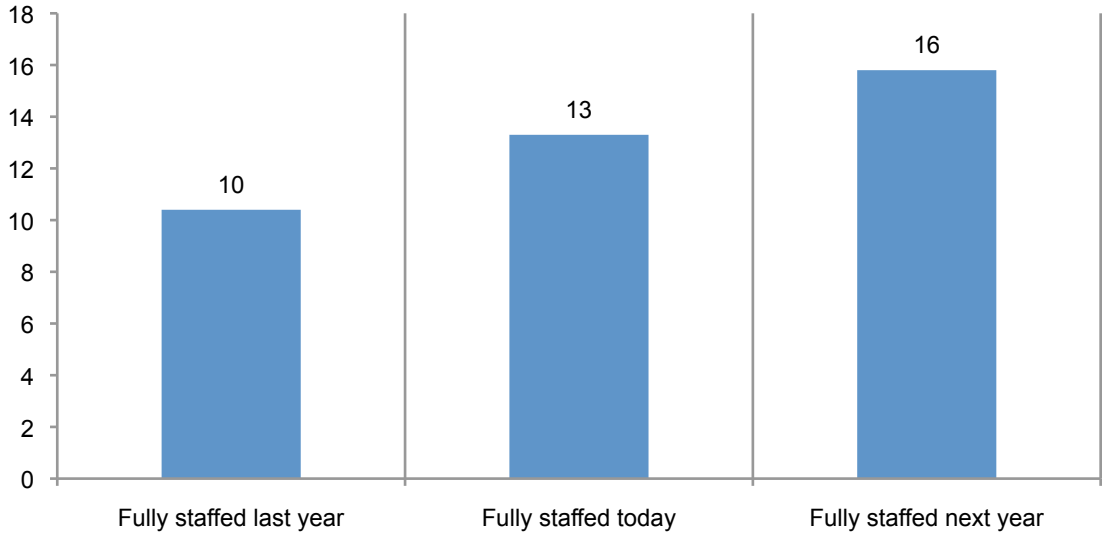


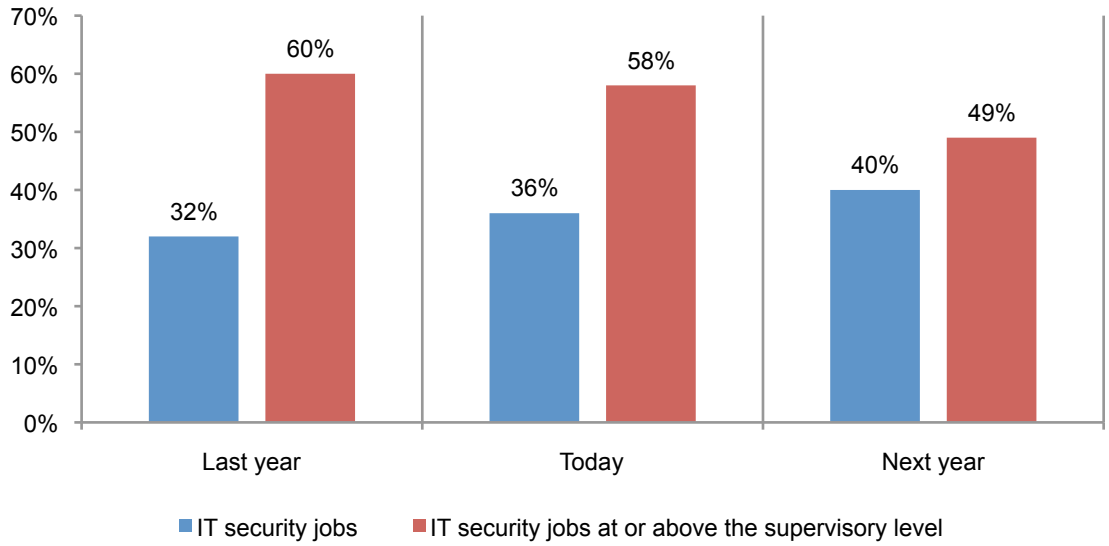
Figure 3 reveals trends in the hiring of IT security specialists who are at or above the supervisory level in their organizations. Last year the average was 10 senior level employees and it increased to 13 who are at the supervisory level or higher. Next year the total average headcount is expected to grow to 16.

Figure 3. Average number of senior IT security professionals in security functions



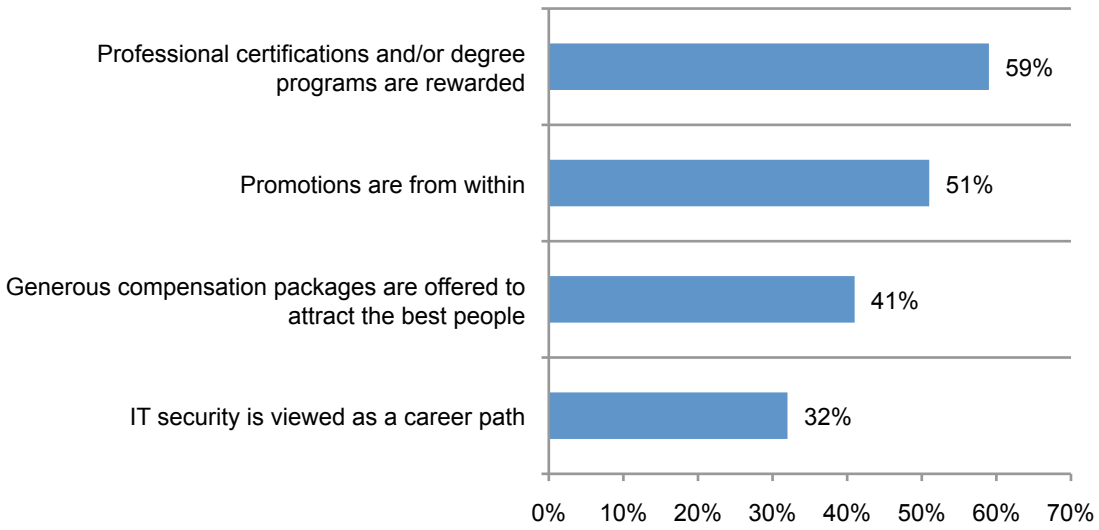
Despite anticipated increases in hiring, the number of positions left unfilled (vacancy rate) increases as well. This suggests the demand for IT security specialists is not being met. As shown in Figure 4, the average vacancy rate increased from 32 percent to 36 percent. Next year it is expected to grow to an average of 40 percent. The percentage of unfilled senior level security experts indicates that organizations are having a hard time filling these positions. However, there is a slight decrease in vacancy rates in the coming year.

Figure 4. Average percentage of IT security positions not filled



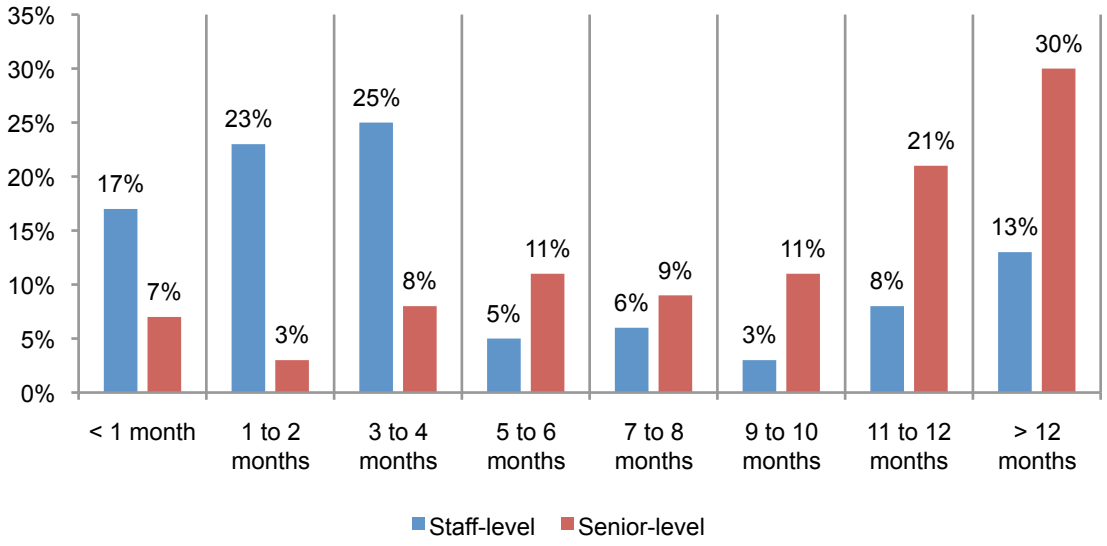
Why is recruiting and retaining IT security personnel difficult? Figure 5 reveals two reasons why staffing may be a challenge. First, 59 percent of respondents (100-41 percent) do not agree that their organizations are offering generous compensation packages to attract the best-qualified people. Second, the IT security function in many organizations can be considered a dead-end job. Only 32 percent of respondents say their organization views IT security as a career path. Slightly more than half (51 percent) of respondents do say their organization promotes from within. However, 59 percent say professional certifications and degree programs are rewarded.

Figure 5. Perceptions about the hiring and promotion of IT security practitioners
Strongly agree and agree response combined



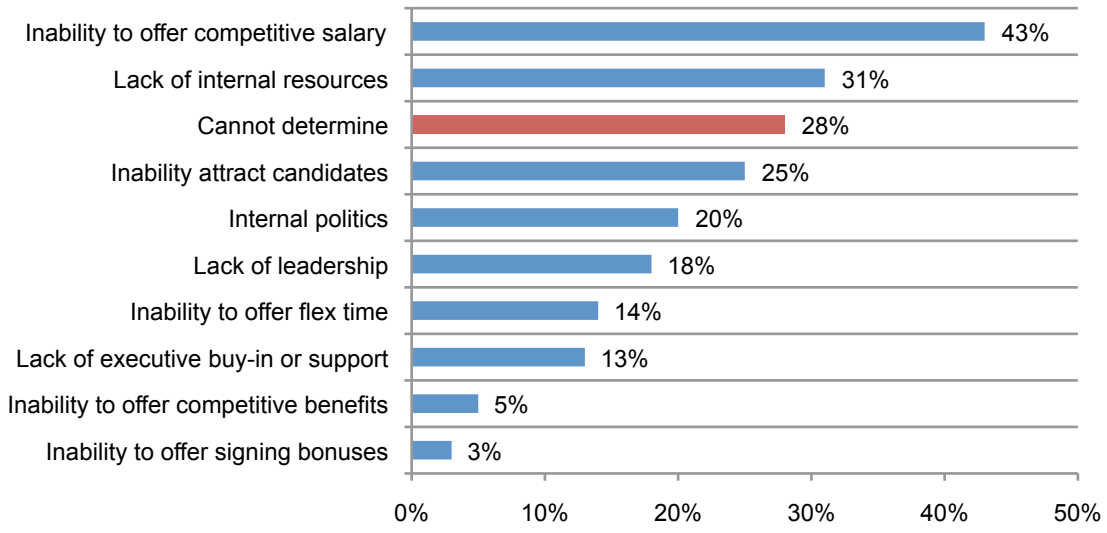
As can be expected, it takes more time to find and hire an experienced security professional. According to Figure 6, a staff level position is typically filled in an average of 5 months. To find a more seasoned executive can take an average of almost a year or 9 months. Forty-eight percent of respondents say their organization gives equal consideration to both internal and external candidates for a position.

Figure 6. Length of time to fill a job requisition
Extrapolated value: staff -level 5.1 months, senior-level 9.2 months



A competitive salary is key to attracting and keeping staff. Organizations represented in this research find it difficult to find or keep staff the main reasons are shown in Figure 7. Primarily it is the inability to offer competitive salaries and lack of internal resources or adequate budget. However, 28 percent cannot determine the reason.

Figure 7. Reasons why positions are unfilled
Two responses permitted



Senior IT specialists are less likely to stay with a company. The average number of years IT security technicians stay in their position is 4, according to Figure 8. However, this drops to 3 years for supervisory and manager-level employees and 2.5 years for director and executive-level employees.

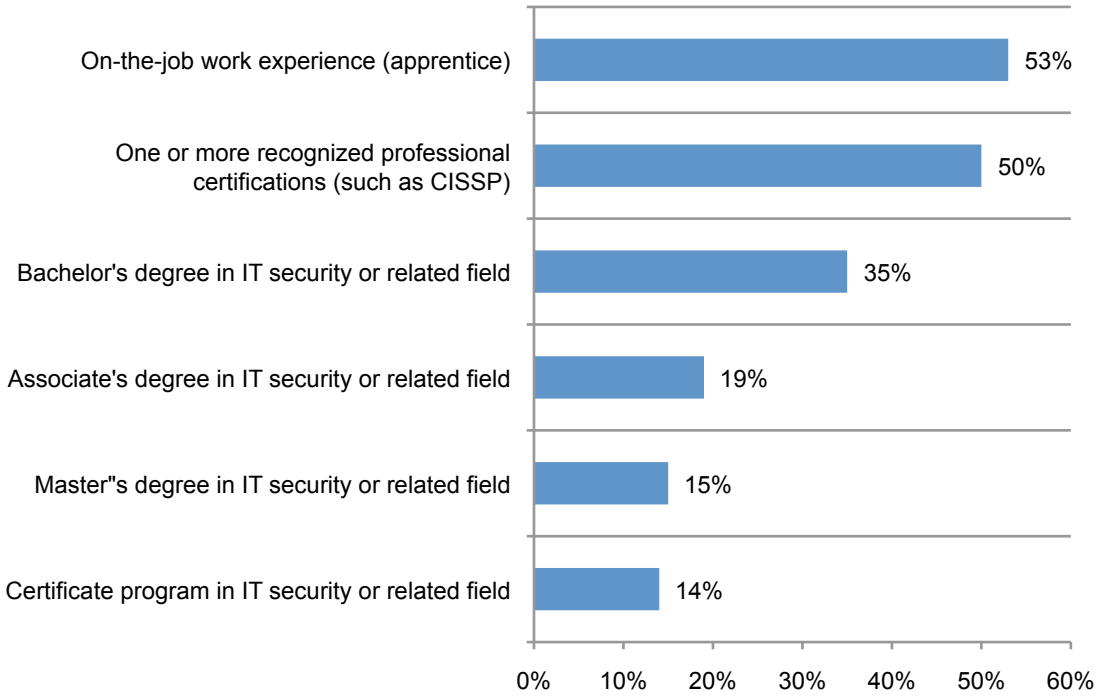
Figure 8. Average length of employment

IT security rarely determines their organization's IT staffing and recruitment strategy. Thirty-four percent of respondents say the human resources function is most responsible for the hiring strategy followed closely by corporate IT (33 percent) and then IT security (21 percent). Forty-four percent of organizations in the study have a CISO or equivalent. Of those, less than half have the final authority on whom to hire.

Actual work experience and certifications are viewed favorably. Figure 9 reveals that more important than a bachelor's degree specializing in IT security or related field is on-the-job work experience and one or more recognized professional certifications.

However, 57 percent say the completion of a recognized college or graduate-level degree program is essential or very important in the hiring decision.

Figure 9. The ideal background for job candidates
More than one response permitted



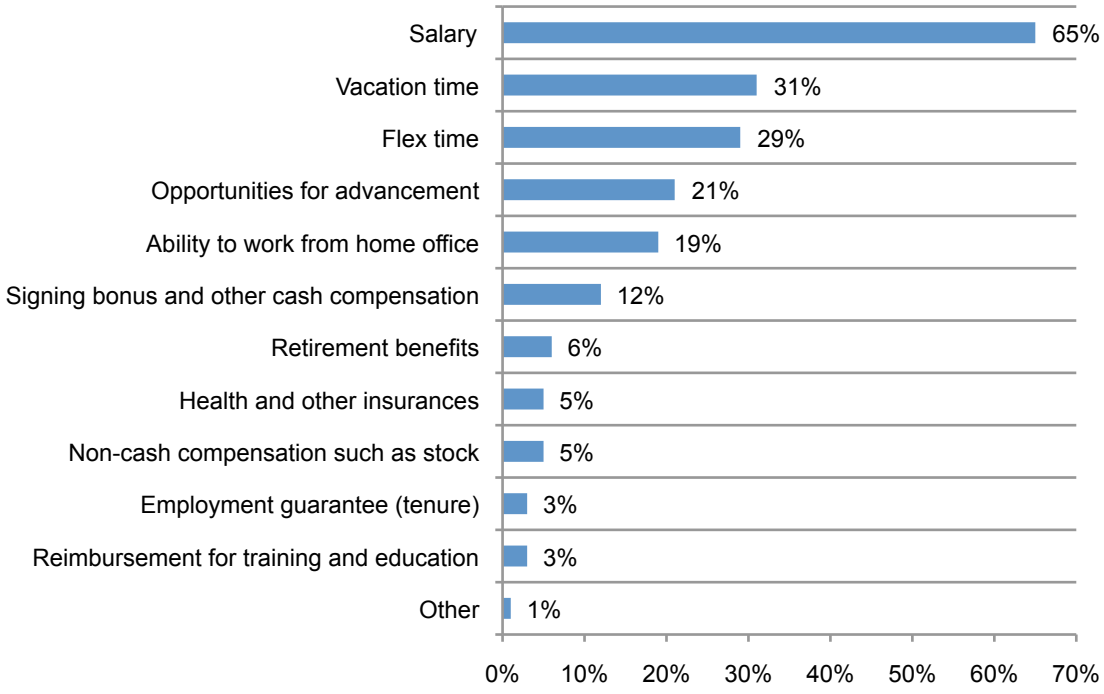
Most job recruiting takes place at conferences (40 percent of respondents) followed by recruitment agencies (34 percent). Thirty percent say they recruit at colleges and universities and another 30 percent say they use social networks.

Salary is most important in attracting job candidates. When asked what they believe is the most important feature in a hiring package, 65 percent of respondents say it is salary, according to Figure 10. This is followed by vacation or personal time (31 percent).

Experienced candidates may be looking for other benefits in addition to salary. These include opportunities for advancement, the ability to work from a home office, signing bonus and other cash compensation and health and other insurances. These are seldom a part of a hiring package.

The findings also reveal that compensation is often higher for IT security than other IT jobs. According to 51 percent of respondents, IT security employees are paid more than other IT jobs and 40 percent say they are paid the same.

Figure 10. Most important features in hiring packages
Two responses permitted



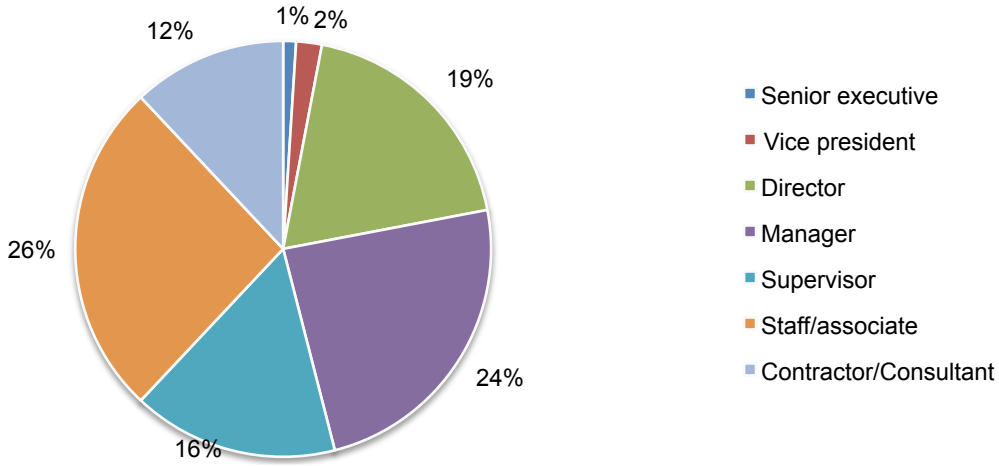
Part 4. Methods

A sampling frame of 14,565 human resources and IT security specialists in the United States were selected as participants to this survey. As shown in Table 1, 551 respondents completed the survey. Screening and failed reliability checks removed 47 surveys. The final sample was 504 surveys or a 3.5 percent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	14,565	100.0%
Total returns	551	3.8%
Rejected and screened surveys	47	0.3%
Final sample	504	3.5%

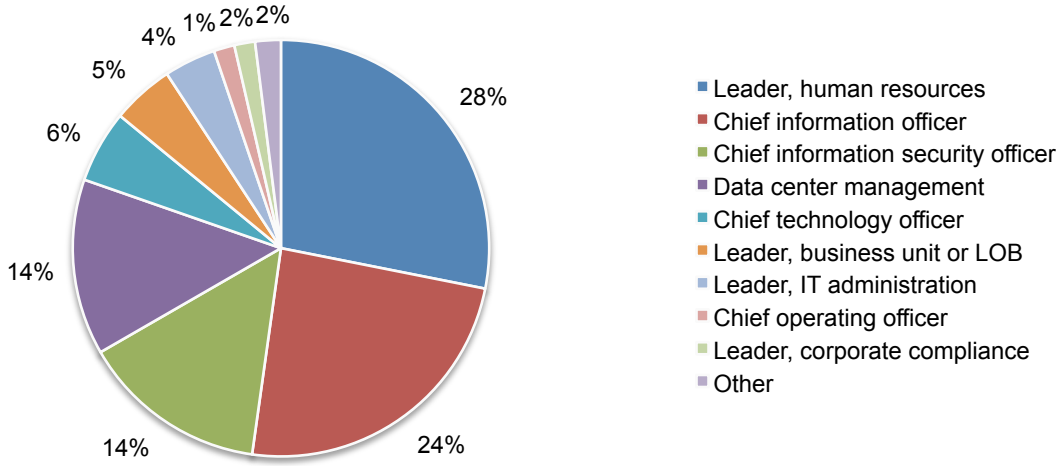
Pie Chart 1 reports the organizational level of respondents' current position. By design, 62 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Organizational level that best describes your current position



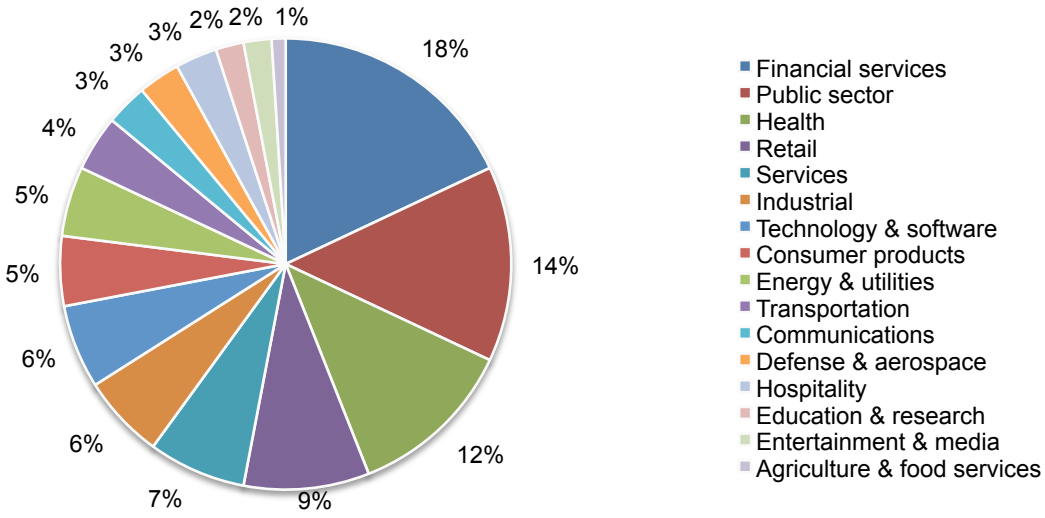
According to Pie Chart 2, 28 percent of respondents report directly to the leader of human resources and 24 percent report to the Chief Information Officer.

Pie Chart 2. Primary person you or your immediate supervisor reports to



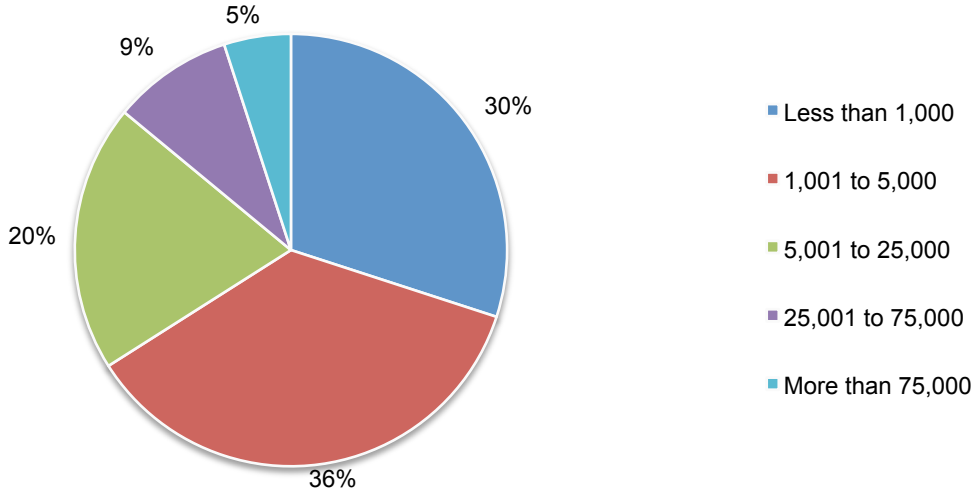
Pie Chart 3 reports the primary sector of the respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (14 percent) and health (12 percent).

Pie Chart 3. What industry best describes your organization's primary sector?



Pie Chart 4 reveals the worldwide headcount of the respondent's organization. Seventy percent of respondents are from organizations with a global headcount greater than 1,000.

Pie Chart 4. Organization's worldwide headcount



Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are human resources or IT security specialist. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2013

Sample response	Freq.	Pct%
Total sampling frame	14,565	100.0%
Total survey returns	551	3.8%
Total rejected or screened surveys	47	0.3%
Final sample	504	3.5%

Part 1. Screening Questions

S1. What best describes your role in attracting, hiring, promoting and retaining IT security personnel within your organization today? Check all that apply.	Pct%
Setting hiring priorities	63%
Recruiting qualified job candidates	58%
Determining job requirements	56%
Evaluating job candidate's performance and fit	53%
Retaining and advancing existing personnel	48%
Setting compensation packages	40%
None of the above (Stop)	0%
Average	45%

S2. How do you rate your level of involvement in recruiting and retaining qualified IT security personnel in your organization?	Pct%
Very high level of involvement	30%
High level of involvement	43%
Moderate level of involvement	27%
Low level or no involvement (Stop)	0%
Total	100%

S3. What best defines your functional role within your organization.	Pct%
I consider myself a human resources (HR) specialist	54%
I consider myself an IT security specialist	23%
I am both an HR and IT security specialist	23%
None of the above (Stop)	0%
Total	100%

Part 2. Attributions. Strongly agree and Agree responses	Strongly agree	Agree
Q1a. My organization has no difficulty **attracting** qualified candidates	15%	19%
Q1b. My organization has no difficulty **retaining** qualified candidates	19%	23%
Q1c. My organization's IT security function is typically understaffed	33%	37%
Q1d. My organization typically promotes from within	26%	25%
Q1e. My organization rewards those who seek professional certifications and/or degree programs	29%	30%
Q1f. My organization offers generous (market-leading) compensation packages to attract the best people	20%	21%
Q1g. My organization views IT security as a career path	14%	18%

Part 3. General Questions

Q2. Approximately, what is the total headcount of IT security specialists in your organization? Please include open job requisitions in your estimates.		
Fully staffed **today**	Pct%	
Less than 5	12%	
5 to 10	33%	
11 to 20	21%	
21 to 30	12%	
31 to 40	8%	
41 to 50	7%	
51 to 100	3%	
More than 100	4%	Headcount
Total	100%	22.0

Fully staffed **last year**	Pct%	
Less than 5	16%	
5 to 10	39%	
11 to 20	16%	
21 to 30	11%	
31 to 40	9%	
41 to 50	5%	
51 to 100	2%	
More than 100	2%	Headcount
Total	100%	18.0

Fully staffed **next year**	Pct%	
Less than 5	8%	
5 to 10	25%	
11 to 20	20%	
21 to 30	15%	
31 to 40	11%	
41 to 50	8%	
51 to 100	6%	
More than 100	7%	Headcount
Total	100%	28.9

Q3. Approximately, what is the headcount of IT security specialists **who are at or above the supervisory level** in your organization? Please include open job requisitions in your estimates.		
Fully staffed **today**	Pct%	
Less than 5	22%	
5 to 10	40%	
11 to 20	26%	
21 to 30	5%	
31 to 40	3%	
41 to 50	1%	
51 to 100	2%	
More than 100	1%	Headcount
Total	100%	13.3

Fully staffed **last year**	Pct%	
Less than 5	30%	
5 to 10	39%	
11 to 20	25%	
21 to 30	2%	
31 to 40	2%	
41 to 50	1%	
51 to 100	1%	
More than 100	0%	Headcount
Total	100%	10.4

Fully staffed **next year**	Pct%	
Less than 5	16%	
5 to 10	32%	
11 to 20	26%	
21 to 30	18%	
31 to 40	4%	
41 to 50	2%	
51 to 100	1%	
More than 100	1%	Headcount
Total	100%	15.8

Q4. Approximately, what is the percentage of IT security jobs that remain open and unfilled?		
Percentage openings **today**	Pct%	
Less than 5%	8%	
5 to 10%	15%	
11 to 20%	16%	
21 to 30%	11%	
31 to 40%	12%	
41 to 50%	20%	
More than 50%	18%	Vacancy rate
Total	100%	36%

Percentage openings **last year**	Pct%	
Less than 5%	24%	
5 to 10%	15%	
11 to 20%	9%	
21 to 30%	8%	
31 to 40%	10%	
41 to 50%	12%	
More than 50%	22%	Vacancy rate
Total	100%	32%

Percentage openings **next year**	Pct%	
Less than 5%	6%	
5 to 10%	12%	
11 to 20%	10%	
21 to 30%	11%	
31 to 40%	15%	
41 to 50%	23%	
More than 50%	23%	Vacancy rate
Total	100%	40%

Q5. Approximately, what is the percentage of IT security jobs **at or above the supervisory level** that remain open and unfilled?		
Percentage openings **today**	Pct%	
Less than 5%	0%	
5 to 10%	3%	
11 to 20%	4%	
21 to 30%	6%	
31 to 40%	11%	
41 to 50%	20%	
More than 50%	56%	Vacancy rate
Total	100%	58%

Percentage openings **last year**	Pct%	
Less than 5%	1%	
5 to 10%	3%	
11 to 20%	2%	
21 to 30%	5%	
31 to 40%	7%	
41 to 50%	20%	
More than 50%	62%	Vacancy rate
Total	100%	60%

Percentage openings **next year**	Pct%	
Less than 5%	4%	
5 to 10%	6%	
11 to 20%	8%	
21 to 30%	8%	
31 to 40%	13%	
41 to 50%	21%	
More than 50%	40%	Vacancy rate
Total	100%	49%

Q6. What are the main reasons for the vacancy rates (if any) determined above? Please select only two top choices.	Pct%
Inability to offer competitive salary'	43%
Lack of internal resources	31%
Cannot determine	28%
Inability attract candidates	25%
Internal politics	20%
Lack of leadership	18%
Inability to offer flex time	14%
Lack of executive buy-in or support	13%
Inability to offer competitive benefits	5%
Inability to offer signing bonuses	3%
Other	0%
Total	200%

Q7. Approximately, what is the average length of employment or tenure for IT security personnel in your organization over the past few years?		
Technicians and staff level employees	Pct%	
Less than 1 year	0%	
1 year	13%	
2 years	11%	
3 years	18%	
4 years	18%	
5 years	21%	
6 years	8%	
7 years	5%	
8 years	2%	
9 years	1%	
10 years	2%	
More than 10 years	1%	Tenure
Total	100%	4.1

Supervisory and manager-level employees	Pct%	
Less than 1 year	0%	
1 year	22%	
2 years	20%	
3 years	24%	
4 years	16%	
5 years	8%	
6 years	3%	
7 years	3%	
8 years	1%	
9 years	0%	
10 years	2%	
More than 10 years	1%	Tenure
Total	100%	3.2

Director and executive-level employees	Pct%	
Less than 1 year	3%	
1 year	30%	
2 years	31%	
3 years	12%	
4 years	11%	
5 years	7%	
6 years	2%	
7 years	3%	
8 years	0%	
9 years	0%	
10 years	1%	
More than 10 years	0%	Tenure
Total	100%	2.5

Q8a. On average, how long does it take to fill a job requisition for a **staff-level employee** in the IT security department or function?	Pct%	
Less than 1 month	17%	
1 to 2 months	23%	
3 to 4 months	25%	
5 to 6 months	5%	
7 to 8 months	6%	
9 to 10 months	3%	
11 to 12 months	8%	
More than 12 months	13%	Months
Total	100%	5.1

Q8b. On average, how long does it take to fill a job requisition for an executive or senior-level employee in the IT security department or function?	Pct%	
Less than 1 month	7%	
1 to 2 months	3%	
3 to 4 months	8%	
5 to 6 months	11%	
7 to 8 months	9%	
9 to 10 months	11%	
11 to 12 months	21%	
More than 12 months	30%	Months
Total	100%	9.2

Q9. What best describes your organization's priorities for hiring qualified IT security personnel?	Pct%
Internal and external candidates are equal priorities	48%
Prioritize qualified external candidates	25%
Prioritize qualified internal candidates	23%
Cannot determine	4%
Total	100%

Q10. What best describes the operating structure of your organization's IT security function or department?	Pct%
Centralized operations for the entire company	43%
Centralized operations within business units or lines of business	26%
Hybrid (combination) of decentralized and centralized operations	19%
Decentralized operations within business units or lines of business	10%
Other	2%
Total	100%

Q11a. Does your organization have a chief information security officer (CISO or equivalent title)?	Pct%
Yes	44%
No	56%
Total	100%

Q11b. If yes, does the CISO have final authority on whom to hire?	Pct%
Yes	49%
No	51%
Total	100%

Q11c. If yes (Q8a), who is the CISO's direct report?	Pct%
Chief information officer	56%
Dual reporting	24%
Chief operating officer	8%
General manager or LOB leader	5%
Chief financial officer	4%
Chief executive officer	2%
Other	1%
Total	100%

Q12. Who determines the IT security staffing and recruitment strategy in your organization?	Pct%
Human resources	34%
Corporate IT (CIO organization)	33%
IT security	21%
Business unit or LOB leaders	6%
Compliance	4%
Other	2%
Total	100%

Q13. What is the minimum educational requirement for potential new hires?	Pct%
On-the-job work experience (apprentice)	53%
One or more recognized professional certifications (such as CISSP)	50%
Bachelors degree specializing in IT security or directly related field	35%
None of the above are required	24%
Associates degree specializing in IT security or directly related field	19%
Masters degree specializing in IT security or directly related field	15%
Certificate program specializing in IT security or directly related field	14%
Total	210%

Q14. How does your organization find qualified candidates for IT security positions? Please check the top two.	Pct%
Conferences	40%
Recruitment agencies	34%
College/university recruitment	30%
Social networks	30%
Referrals	25%
Ads	21%
Job fairs	18%
Other	2%
Total	200%

Q15a. How important is the completion of a recognized college or graduate-level degree program in the hiring decision?	Pct%
Essential	14%
Very important	43%
Important	27%
Not important	11%
Irrelevant	5%
Total	100%

Q15b. If you said essential, very important or important, please select the names of the institutions you normally recruit qualified candidates in IT security. [Pull-down list provided]

Q16. What are the most important features in hiring packages for IT security professionals? Please check the top two.	Pct%
Salary	65%
Vacation (personal) time	31%
Flex time	29%
Opportunities for advancement	21%
Ability to work from home office	19%
Signing bonus and other cash compensation	12%
Retirement benefits	6%
Non-cash compensation such as stock	5%
Health and other insurances	5%
Reimbursement for training and education	3%
Employment guarantee (tenure)	3%
Other	1%
Total	200%

Q17. Are IT security employees in your organization paid more than, less than or equal to other IT employees?	Pct%
Paid more	51%
Paid equally	40%
Paid less	5%
Unsure	4%
Total	100%

Q18. How would you describe your organization's overall ability to recruit and retain qualified IT security personnel? Your best guess is welcome.	Pct%	
1 and 2 (not effective)	5%	
3 and 4	21%	
5 and 6	29%	
7 and 8	30%	
9 and 10 (very effective)	15%	Effectiveness
Total	100%	6.1

Part 4. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior executive	1%
Vice president	2%
Director	19%
Manager	24%
Supervisor	16%
Staff/associate	26%
Contractor/Consultant	12%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	Pct%
CEO/executive committee	0%
Chief operating officer	2%
Chief information officer	24%
Chief information security officer	15%
Chief technology officer	6%
Chief financial officer	1%
Leader, human resources	28%
Leader, business unit or LOB	5%
Leader, corporate compliance	2%
Leader, risk management	1%
Leader, IT administration	4%
Data center management	14%
Other	0%
Total	100%

D3. Experience	Mean	Median
Total years of relevant experience	9.76	10.00
Total years in current position	5.17	5.50

D4. What industry best describes your organization's primary sector?	Pct%
Financial services	18%
Public sector	14%
Health	12%
Retail	9%
Services	7%
Industrial	6%
Technology & software	6%
Consumer products	5%
Energy & utilities	5%
Transportation	4%
Communications	3%
Defense & aerospace	3%
Hospitality	3%
Education & research	2%
Entertainment & media	2%
Agriculture & food services	1%
Other	0%
Total	100%

D5. What best describes your organization's geographic footprint?	Pct%
Domestic only	15%
Primarily one global region	16%
Primarily two or more global regions	28%
All global regions (multinational)	41%
Total	100%

D6. What is the worldwide headcount of your organization?	Pct%	
Less than1,000	30%	
1,001 to 5,000	36%	
5,001 to 25,000	20%	
25,001 to 75,000	9%	
More than 75,000	5%	Headcount
Total	100%	12,670

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.