Staffing the IT Security Function in the Age of Automation

Sponsored by DomainTools

Independently conducted by Ponemon Institute LLC

Publication Date: May 2018

Staffing the IT Security Function in the Age of Automation

Prepared by Ponemon Institute, May 2018

Part 1. Introduction

Ponemon Institute, with sponsorship from DomainTools, conducted the study *Staffing the IT Security Function in the Age of Automation* to better understand how companies are addressing the need to hire and retain qualified IT security practitioners and the effects automation and artificial intelligence (AI) will have on staffing. Ponemon Institute conducted a similar study in 2013. Whenever possible, this report will show research findings from the previous study.

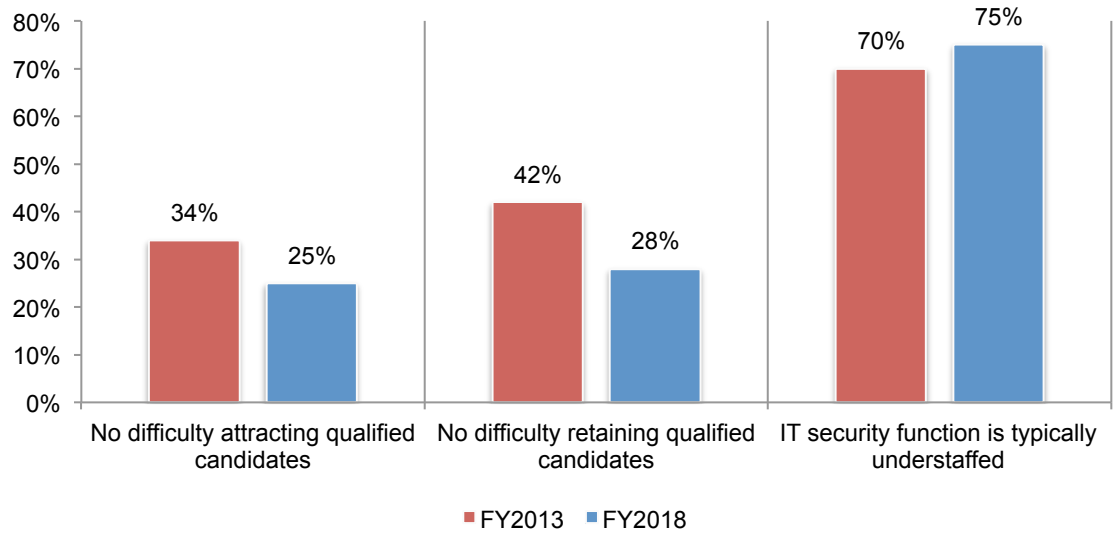
IT security functions continue to be understaffed and at risk. One of the biggest barriers to a strong security posture, according to Ponemon Institute research, is not having a team of security professionals that can deal with complex and serious internal and external threats to the organization. Unfortunately improvements in staffing are not happening.

More than 600 IT and IT security practitioners who participate in attracting, hiring, promoting and retaining IT security personnel within their companies were surveyed. Figure 1 reveals why respondents believe companies are falling behind in keeping IT security functions adequately staffed.

Specifically, only 25 percent of respondents say their organizations **have no difficulty** attracting qualified candidates, compared to 34 percent in 2013. Only 28 percent report their organizations **have no difficulty** retaining qualified candidates compared to 42 percent of respondents in 2013. As a result, more respondents in this year's study say their IT security functions are understaffed than in 2013 (70 percent vs. 75 percent).

Figure 1. Trends in staffing the IT security function

Strongly agree and Agree responses combined



Part 2. Key findings

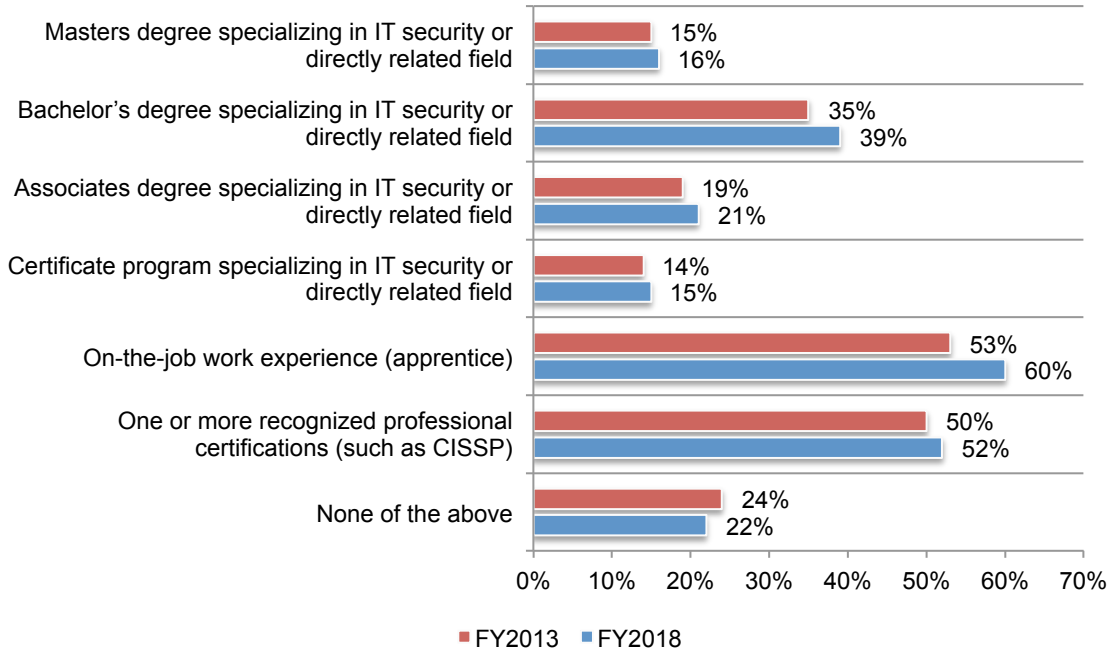
This section presents a detailed analysis of the research. The complete audited findings are presented in the Appendix of this report, which is organized according to the following topics:

- Technical skills and general knowledge in demand
- The effects of automation on IT security staffing
- How to improve the ability to attract and retain qualified personnel
- How to succeed in the age of automation

Technical skills and general knowledge in demand

On-the-job experience is more in demand than a degree. According to Figure 2, more respondents in this year's study (60 percent) say when they are hiring, hands-on experience is desirable. This is followed by one or more recognized professional certifications, such as the CISSP).

Figure 2. What is the minimum educational requirement for job candidates?
More than one response permitted

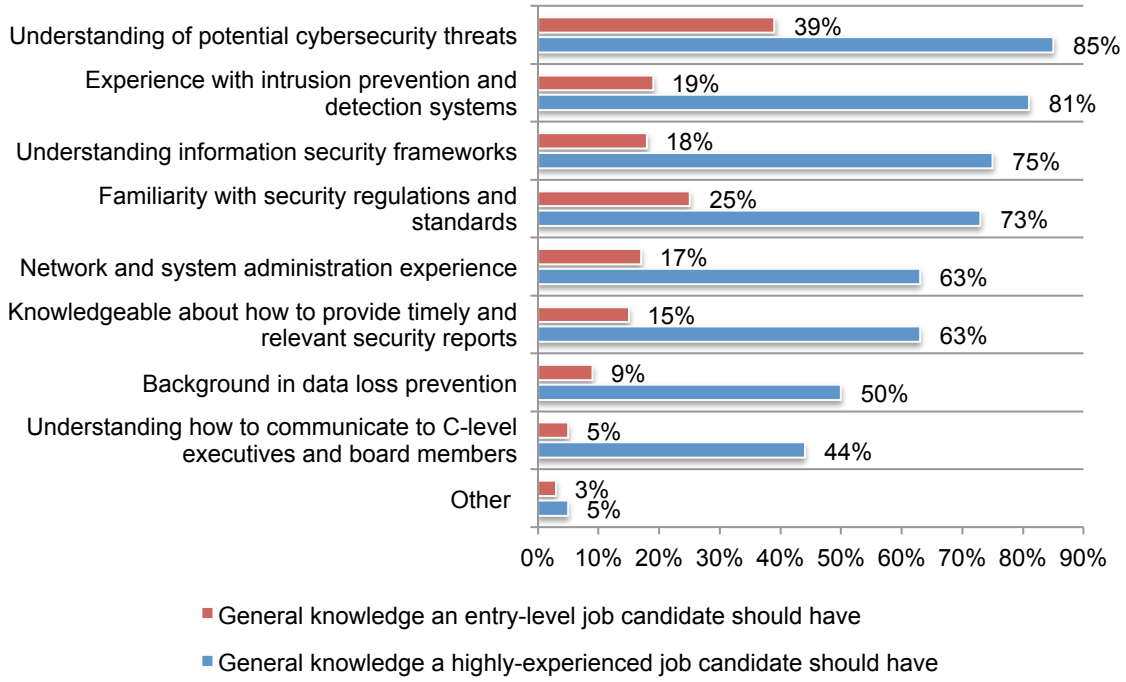


An understanding of potential cybersecurity threats is important for entry-level and highly experienced job candidates. Understandably, as shown in Figure 3, respondents say their organizations have great expectations that highly experienced job candidates will bring more general knowledge to their positions.

The top three categories of general knowledge for entry-level candidates are an understanding of potential cybersecurity threats, familiarity with security regulations and standards and experience with intrusion prevention and detection systems (39 percent, 25 percent and 19 percent of respondents, respectively).

Similarly, highly experienced job candidates are expected to have an understanding of potential cybersecurity threats, experience with intrusion prevention and detection systems and an understanding of information security frameworks (85 percent, 81 percent and 75 percent of respondents, respectively).

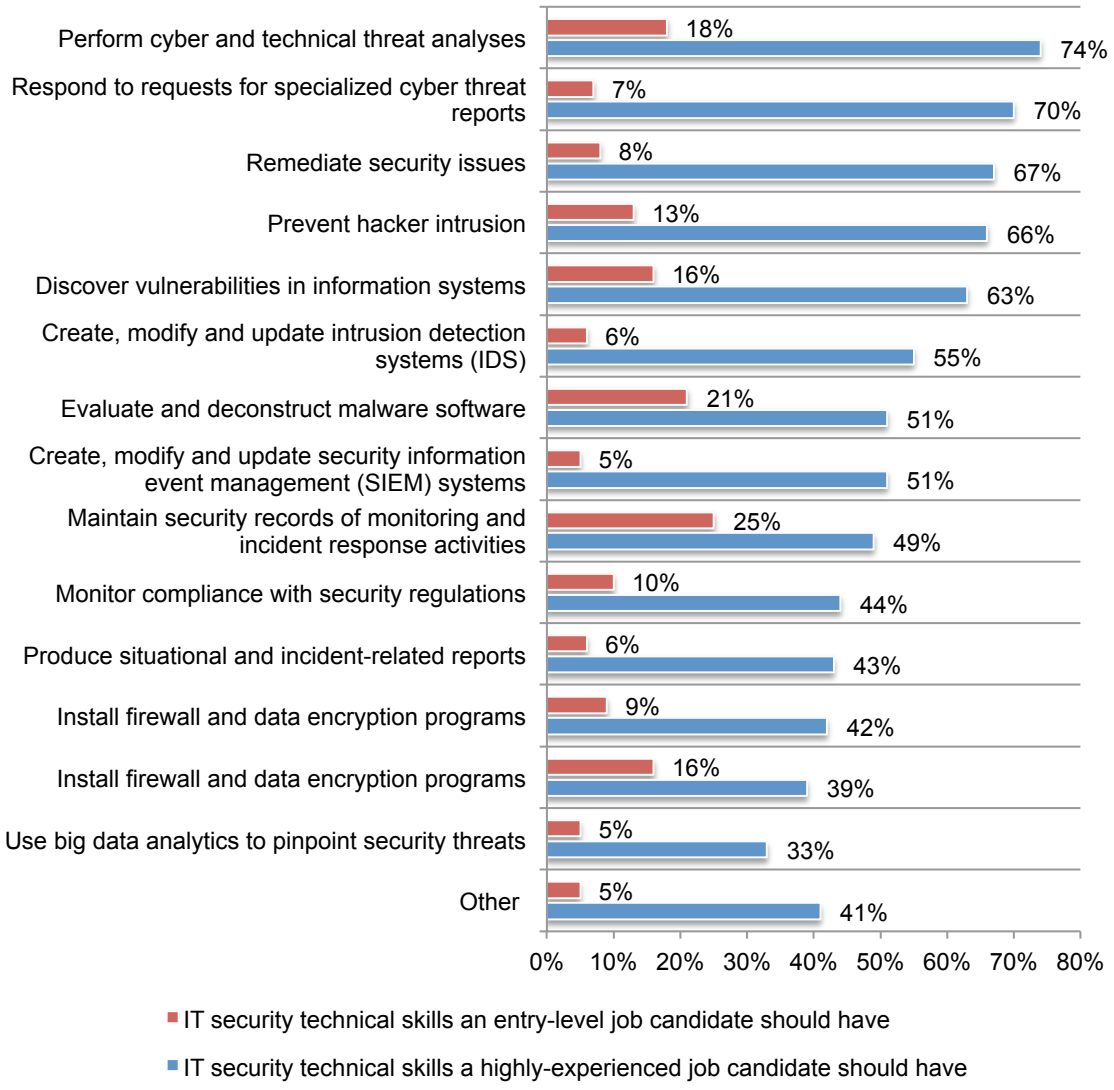
Figure 3. What knowledge should entry-level and highly experienced job candidates have?
More than one response permitted



Experienced job candidates should be able to perform cyber and technical threat analyses. According to Figure 4, only 18 percent of respondents expect entry-level candidates to perform cyber and technical threat analyses. However, 74 percent of respondents say highly experienced candidates are expected to have this skill.

Entry-level candidates are expected to maintain security records of monitoring and incident response activities and evaluate and deconstruct malware software (25 percent and 21 percent of respondents, respectively). Experienced candidates are expected to respond to requests for specialized cyber threat reports and remediate security issues (70 percent and 67 percent of respondents, respectively).

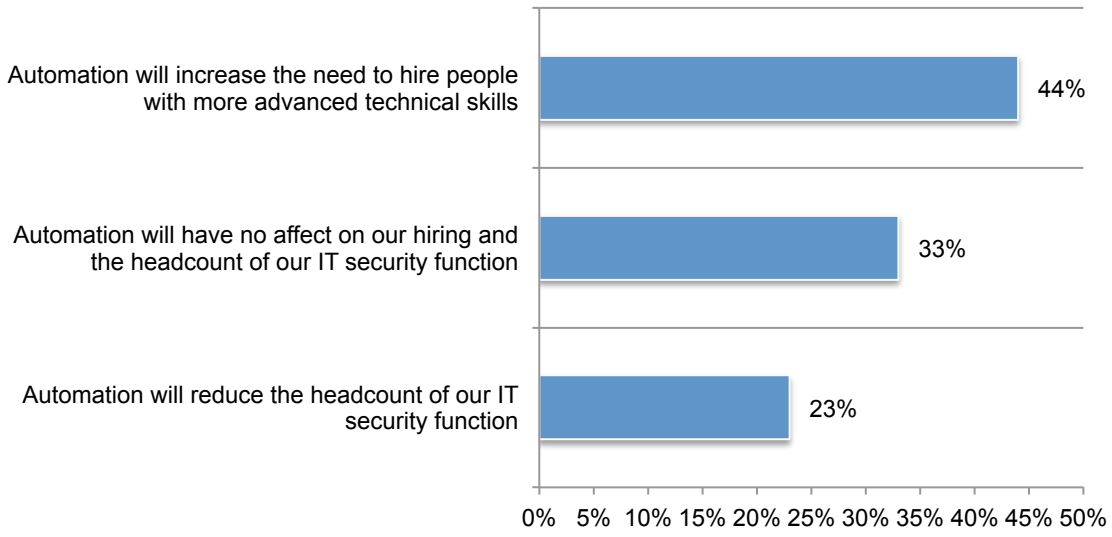
Figure 4. The IT security technical skills entry-level and highly experienced job candidates should have
More than one response permitted



The effect of automation on IT security staffing

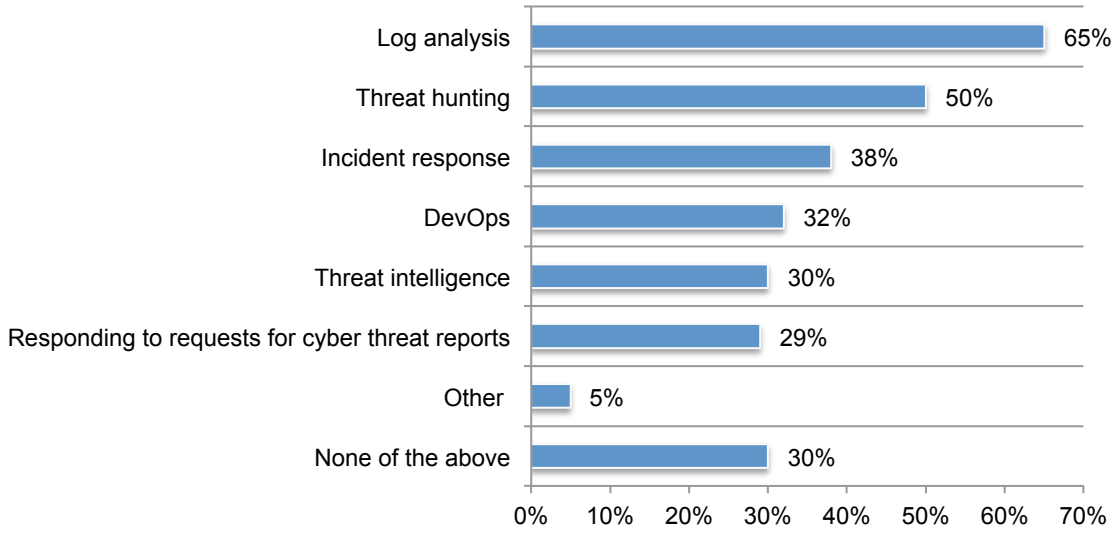
Automation will not reduce the need for IT security professionals. As shown in Figure 5, 44 percent of respondents predict automation will increase the need to hire people with more advanced skills. Only 23 percent of respondents say automation will reduce the head count of their IT security function.

Figure 5. How will automation affect the hiring of IT security personnel?



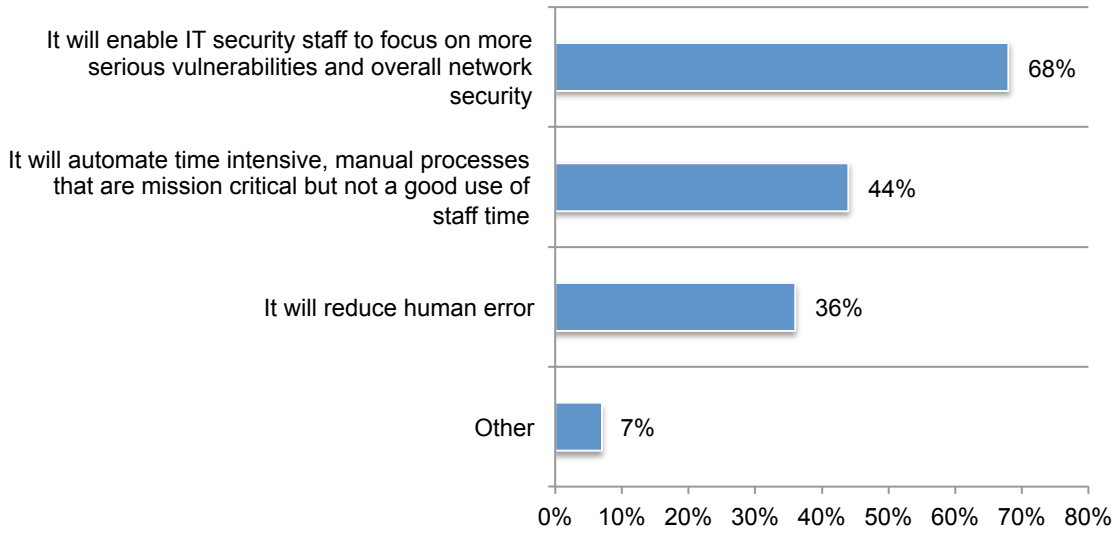
Log analysis activities will be automated. Seventy-two percent of respondents say their organizations use automation (26 percent) or expect to use it in the next six to 12 months (46 percent). As shown in Figure 6, these respondents expect log analysis (65 percent) and threat hunting (50 percent) to be automated. Only 29 percent of respondents expect responding to requests for cyber threat reports will be automated.

Figure 6. What activities currently performed by your IT security staff will automation replace?
More than one response permitted



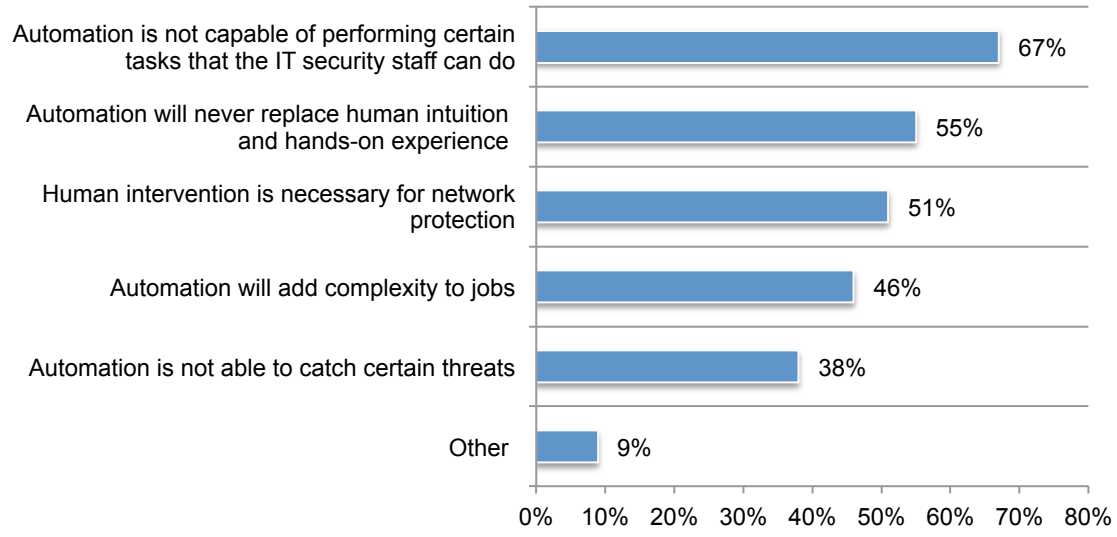
Automation will enable IT security staff to focus on more serious threats. Sixty percent of respondents in organizations that will deploy automation believe it will improve their IT security staffs' ability to do their jobs because it will enable them to focus on more serious vulnerabilities and overall network security (68 percent of respondents). Forty-four percent of respondents say it will automate time intensive, manual processes that are mission critical but not a good use of staff time, according to Figure 7. Only 25 percent of respondents believe they will lose their jobs as a result of automation.

Figure 7. How will automation improve the ability of their IT security staff to do their jobs?
More than one response permitted



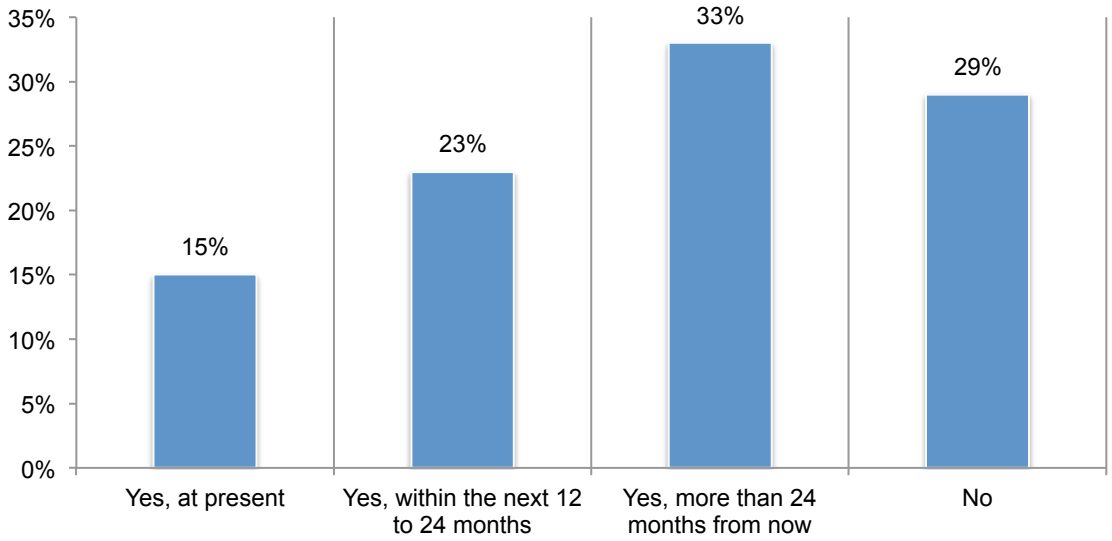
Twenty-eight percent of respondents believe it will **not improve** their IT security staffs' work or are unsure (12 percent). According to Figure 8, these respondents say automation is not capable of performing certain tasks that the IT security staff can do (67 percent) or automation will never replace human intuition and hands-on experience (55 percent)

Figure 8. How will automation not improve your IT security staff's ability to do their job?
More than one response permitted



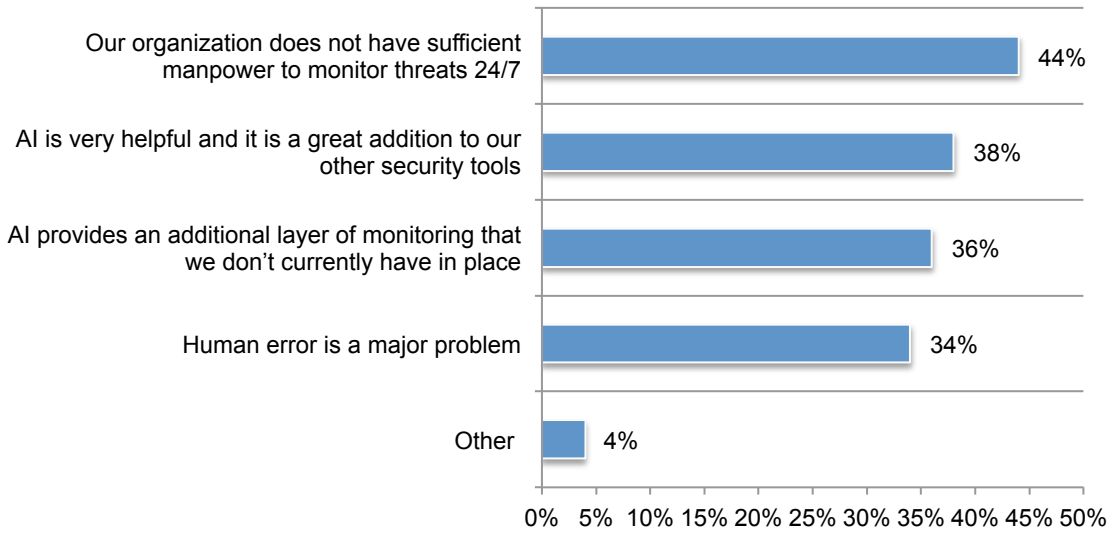
Most organizations believe artificial intelligence (AI) is or will be a dependable and trusted security tool. According to Figure 9, 71 percent of respondents believe AI is a dependable and trusted security tool today (15 percent). As AI becomes more integral to an organization's security strategies over the next two years, 56 percent of respondents say it will be dependable and trusted.

Figure 9. Is AI a dependable and trusted security tool?



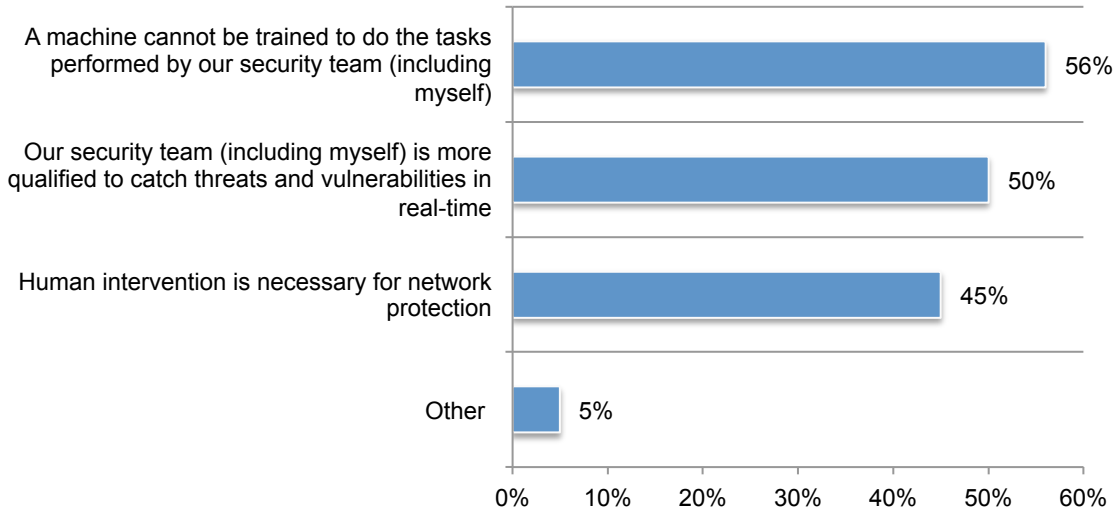
AI is important to monitor threats 24/7. Of the 71 percent of respondents who have a positive view of AI, 44 percent of respondents say their organization does not have sufficient manpower to monitor threats 24/7, and 38 percent say AI is very helpful and is a great addition to their other security tools.

New Figure 10. Why is AI considered dependable and trusted?



Some respondents say AI will not replace the security team. Twenty-nine percent of respondents say AI is not a dependable and trusted security tool for their organizations. As shown in Figure 11, the primary reasons are that a machine cannot be trained to do the tasks performed by their security teams (56 percent of respondents) and the security team is more qualified to catch threats and vulnerabilities in real-time (50 percent of respondents).

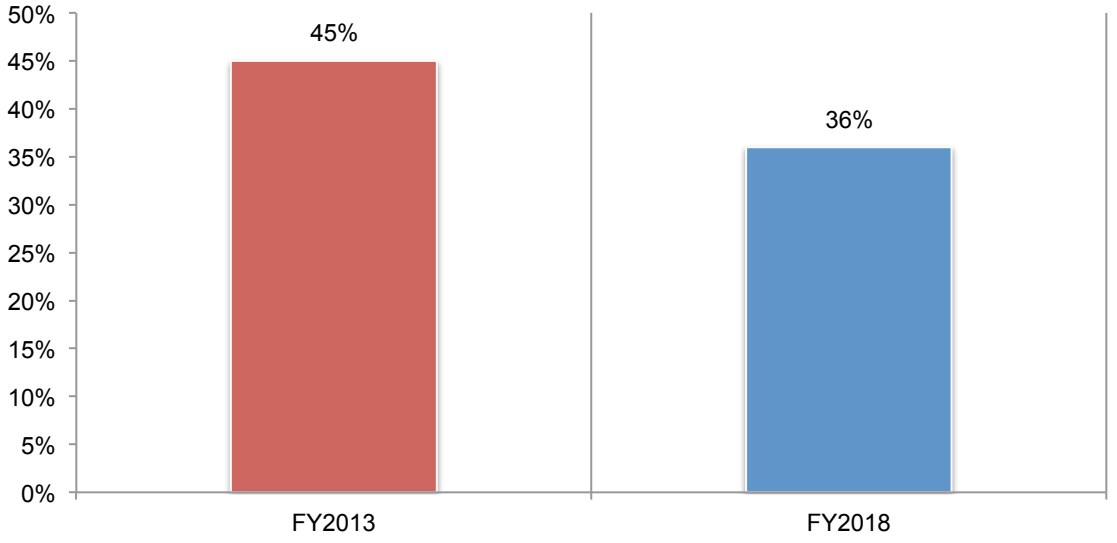
Figure 11. Why is AI not considered a dependable and trusted security tool?
More than one response permitted



How to improve the ability to attract and retain qualified personnel

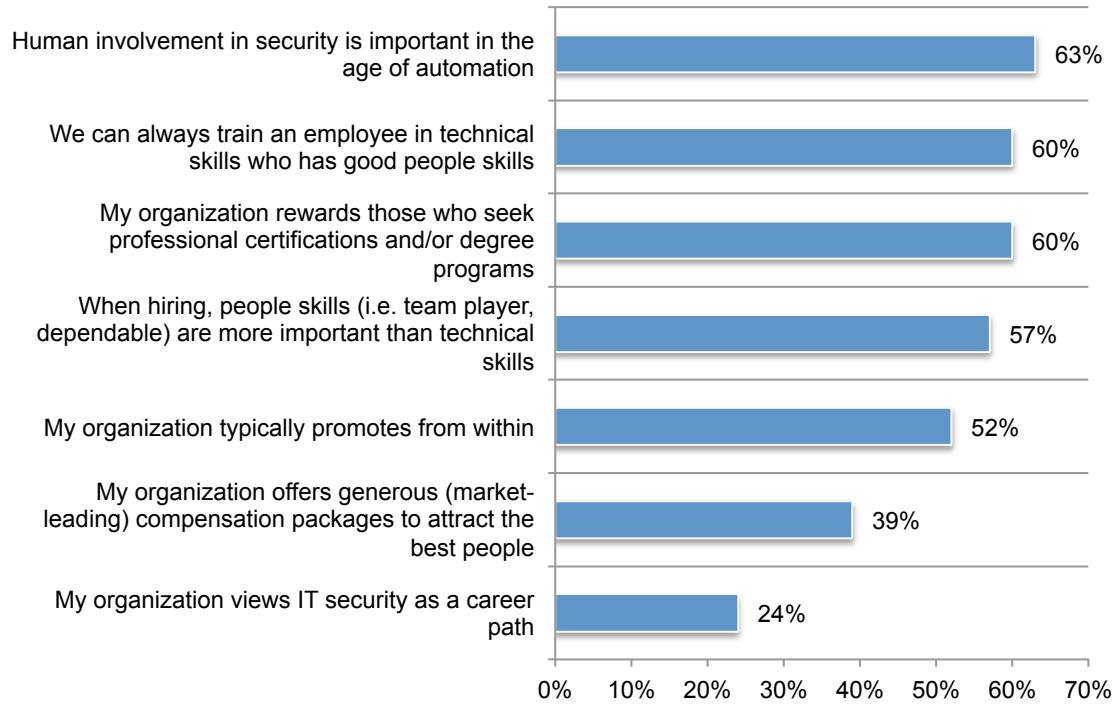
New approaches are needed to improve the ability to recruit and retain qualified IT security staff. When asked to rate their organizations' ability to recruit and retain qualified security staff on a scale of 1 = no ability to 10 = high ability, only 36 percent in this year's study say they have a high ability (response of 7+). In 2013, more respondents were confident in their recruitment and retention practices (45 percent).

Figure 12. How would you rate your organization's ability to recruit & retain qualified IT security personnel?
7+ on a scale of 1 = no ability to 10 = high ability



Organizations should consider offering better compensation practices and a career path. As discussed previously, organizations are not confident in their ability to improve the staffing of the IT security function. Possible reasons are shown in Figure 13. For example, only 24 percent of respondents say their organization views IT security as a career path and only 39 percent of respondents say their organizations offer generous compensation packages to attract the best people. Another reason is that only about half of respondents' organizations (52 percent) are typically promoting from within.

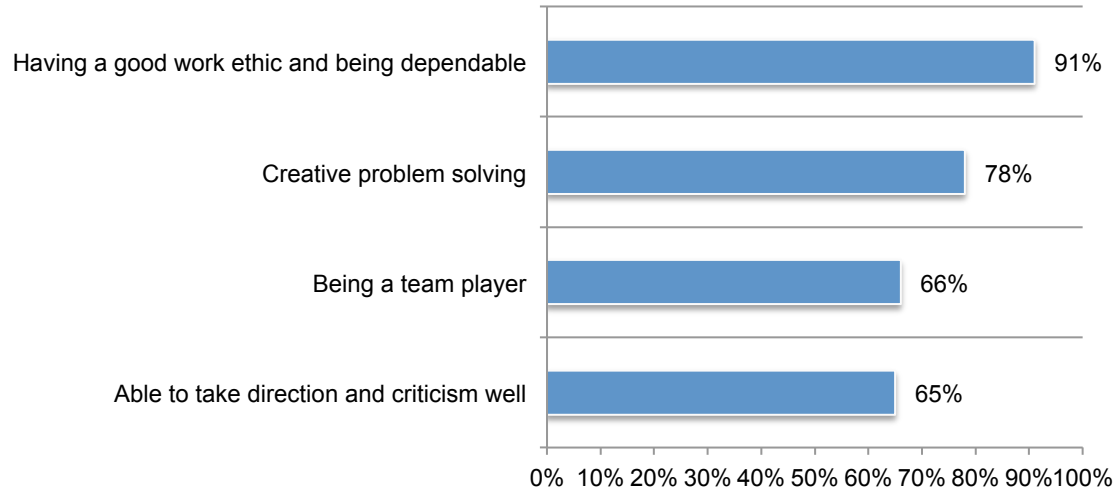
Figure 13. Current practices in hiring and retention of IT security practitioners
Strongly agree and Agree responses combined



How to have a successful career in the age of automation

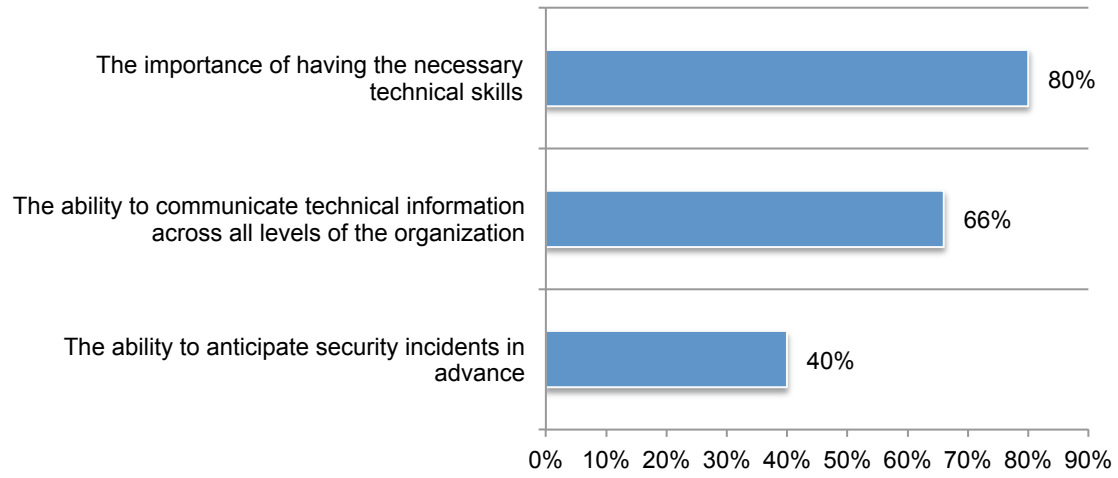
To succeed in IT security, have a good work ethic and be dependable. Respondents were asked to rate seven types of people skills they evaluate on a scale of 1 = not important to 10 = high importance when hiring and promoting IT security personnel. Ninety-one percent of respondents rated having a good work ethic and being dependable as very important, as shown in Figure 14. The following are also considered very important: creative problem solving (78 percent), good communication skills (66 percent), being a team player (66 percent) and the ability to take criticism and direction well (65 percent).

Figure 14. The importance of soft skills
1 = low importance to 10 = high importance, 7+responses reported



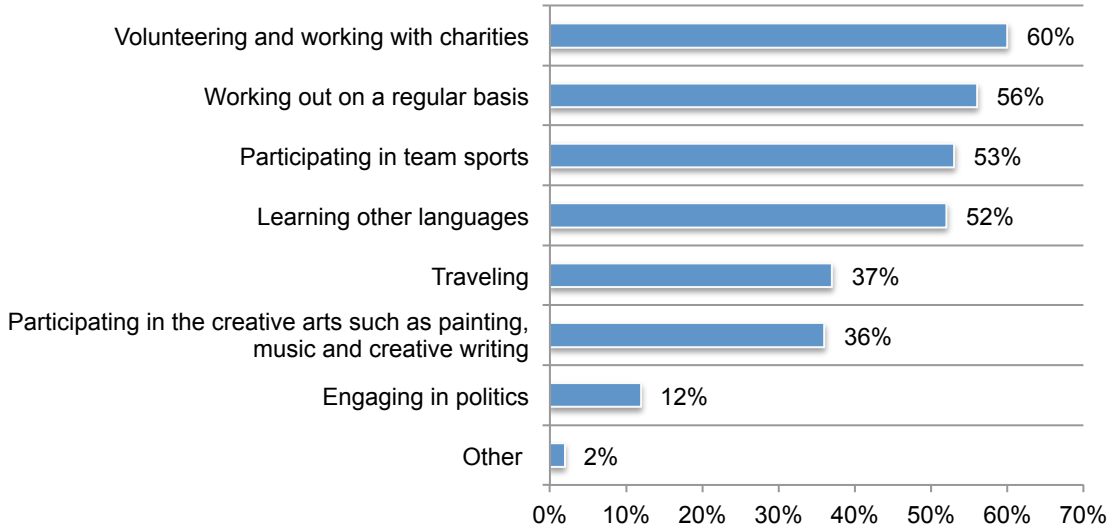
Technical skills are also important. According to Figure 15, 80 percent of respondents say IT security practitioners should have the necessary technical skills, and 66 percent say they should be able to communicate technical information across all levels of the organization.

Figure 15. The importance of technical skills
1 = low importance to 10 = high importance, 7+responses reported



Job candidates should understand how outside interests might improve professional status. Seventy-five percent of respondents say their companies consider a candidate's outside interests important when making a hiring decision. As shown in Figure 16, the three most popular outside interests are volunteering and working with charities (60 percent of respondents), working out on a regular basis (56 percent of respondents) and participating in team sports (53 percent of respondents).

Figure 16. Personal interests matter
More than one response permitted



Conclusion

In addition to revealing the staffing problems companies are experiencing, the research also provides guidance on how to address these challenges. Following are recommendations for organizations and job seekers:

- Compensation matters in attracting and retaining qualified personnel. Because of the competitiveness in the IT security job market, companies should consider offering generous compensation packages to attract and retain the best candidates. The most desirable candidates, according to the study, are those who can bring on-the-job experience and a recognized professional certification (CISSP) to the IT security function.

- Create a career path for IT security staff and promote from within. Most companies represented in this study (76 percent of respondents) do not view IT security as a career path. Companies are at risk of losing their high performers if they do not spend time mentoring and offering opportunities for advancement. Only about half (52 percent of respondents) say their companies promote from within.

- Consider job candidates that may not have all the typical technical skills but have the aptitude, people skills, communication skills and the willingness to be trained. Fifty-seven percent of respondents say that when they are hiring, the softer skills such as being a team player and dependability are more important than technical skills. In fact, 60 percent of respondents say they can always train an employee who has good people skills in technical skills who has good people skills.

- Recognize that investments in automation and AI will not reduce your company's need for skilled IT security personnel. Sixty-three percent of respondents say human involvement in security is important in the age of automation.

- Job candidates should recognize that on-the-job experience, as discussed above, is considered most valuable to potential employers. Ensure that this experience is highlighted in your resume. Also desirable is a recognized professional certification, such as the CISSP. Job candidates should prepare for the age of automation because it will increase the need to hire people with more advanced skills. Only 23 percent of respondents say automation will reduce the head count of their IT security function.

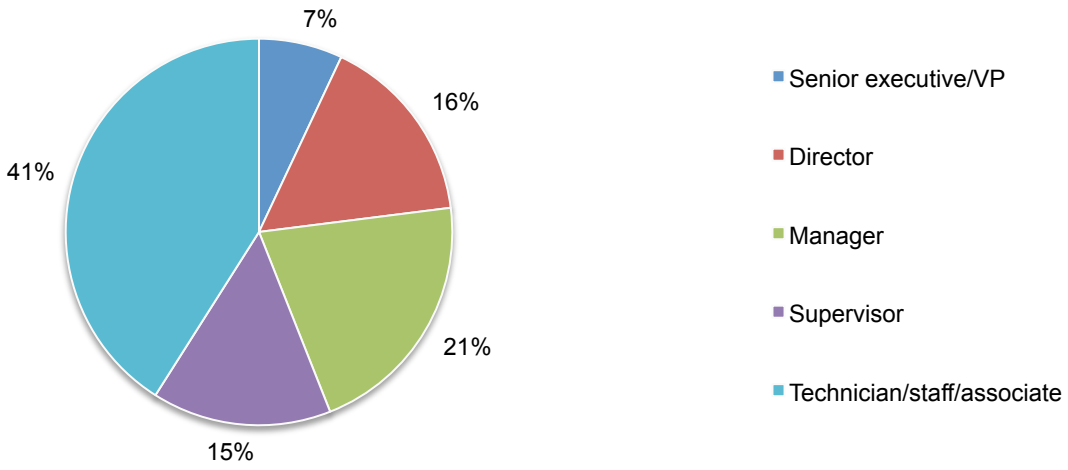
Part 3. Methods

A sampling frame of 16,775 IT and IT security practitioners who participate in attracting, hiring, promoting and retaining IT security personnel in their companies were selected as participants in this survey. Table 1 shows 679 total returns. Screening and reliability checks required the removal of 64 surveys. Our final sample consisted of 615 surveys, or a 3.7 percent response rate.

Table 1. Sample response	FY2017	Pct%
Sampling frame	16,775	100%
Total returns	679	4.0%
Rejected or screened surveys	64	0.4%
Final sample	615	3.7%

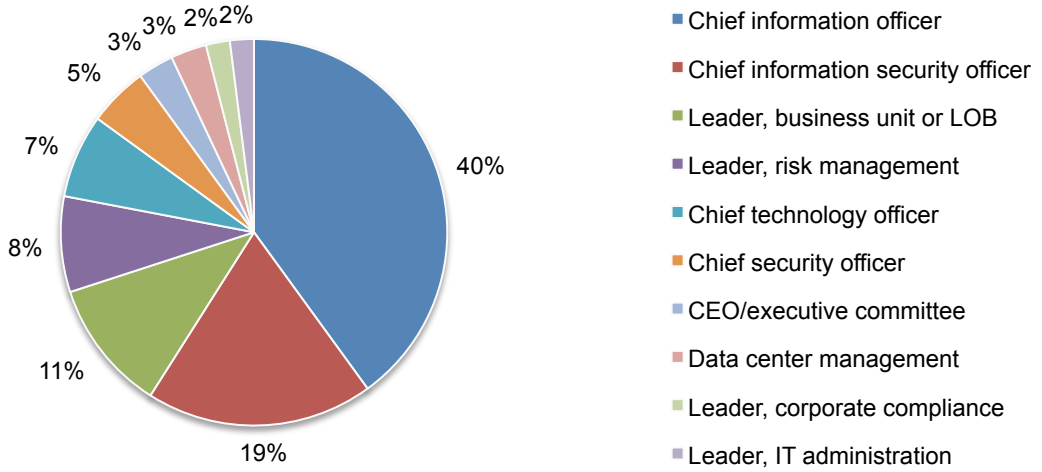
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (59 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



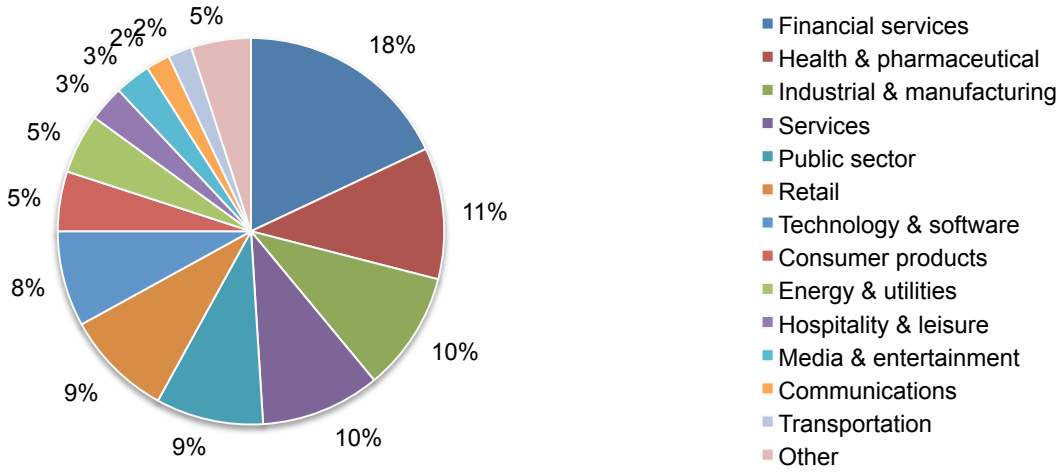
As shown in Pie Chart 2, 40 percent of respondents report to the chief information officer, 19 percent of respondents report to the chief information security officer, 11 percent of respondents report to the business unit leader and 8 percent of respondents indicated they report to the leader of risk management.

Pie Chart 2. Primary person you or your leader reports to



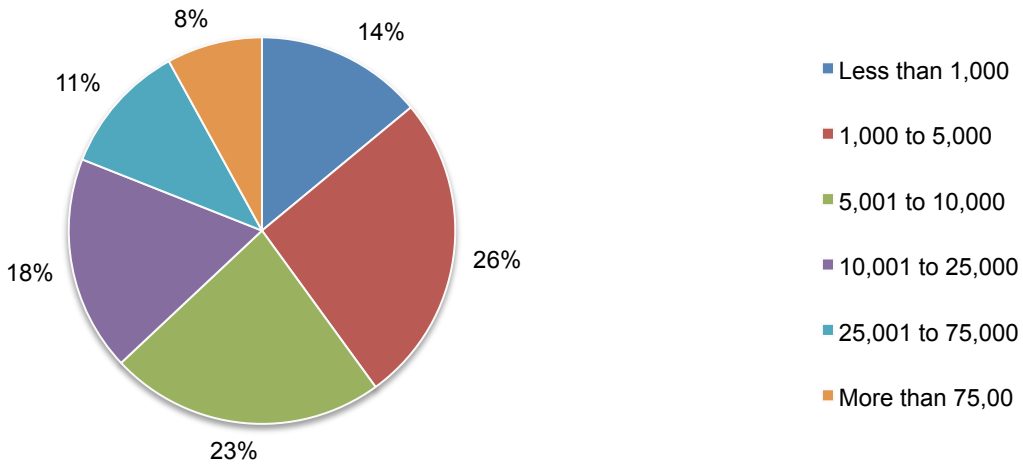
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceuticals (11 percent of respondents), industrial/manufacturing (10 percent of respondents) and the services sector (10 percent of respondents).

Pie Chart 3. Industry distribution of respondents' organizations



Pie Chart 4 reports the worldwide head count of the respondents' organizations. More than half of respondents (60 percent) are from organizations with a worldwide head count greater than 5,000 employees.

Pie Chart 3. Worldwide head count of respondents' organizations



Part 4. Caveats to this study

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 familiar with their organizations' approaches to hiring and retaining IT and IT security personnel. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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, the possibility remains that a subject did not provide accurate responses.

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 February 2018.

Survey response	FY2018	FY2013
Total sampling frame	16,775	14,565
Total returns	679	551
Rejected surveys	64	47
Final sample	615	504
Response rate	3.7%	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.	FY2018
Setting hiring priorities	31%
Determining job requirements	56%
Recruiting qualified job candidates	62%
Evaluating job candidate's performance and fit	60%
Retaining and advancing existing personnel	38%
Setting compensation packages	29%
None of the above (Stop)	0%
Total	276%

S2. What is your primary job function? Please select all that apply.	FY2018
Business continuity/DR	14%
Security analyst	33%
Security architect	19%
Security manager	49%
Incident responder	41%
Risk analyst	26%
IT manager	43%
CISO	20%
CSO	4%
None of the above (Stop)	0%
Total	249%

S3. How do you rate your level of involvement in recruiting and retaining qualified IT security personnel in your organization?	FY2018
Very high level of involvement	40%
High level of involvement	37%
Moderate level of involvement	23%
Low level or no involvement (Stop)	0%
Total	100%

Part 2. The hiring and retention of IT security practitioners in the age of automation

Please rate each one of the following statements about the recruitment of IT security practitioners by your organization using the five-point scale provided below the item. **Strongly agree and Agree response**	FY2018	FY2013
Q1a. My organization has no difficulty **attracting** qualified candidates.	25%	34%
Q1b. My organization has no difficulty **retaining** qualified candidates.	28%	42%
Q1c. My organization's IT security function is typically understaffed.	75%	70%
Q1d. My organization typically promotes from within.	52%	51%
Q1e. My organization rewards those who seek professional certifications and/or degree programs.	60%	59%
Q1f. My organization offers generous (market-leading) compensation packages to attract the best people.	39%	41%
Q1g. My organization views IT security as a career path.	24%	32%
Q1h. My company's use of cyber automation will reduce its need for skilled IT security personnel.	24%	
Q1i. The inability to properly staff skilled security personnel has increased my company's investment in cyber automation tools and technologies.	41%	
Q1j. Human involvement in security is important in the age of automation.	63%	
Q1k. When hiring, people skills (i.e. team player, dependable) are more important than technical skills.	57%	
Q1l. We can always train an employee in technical skills who has good people skills.	60%	

Q2. How would you describe your organization's overall ability to recruit and retain qualified IT security personnel? Your best guess is welcome. Please use the following 10 point scale from 1 = no ability to 10 = high ability.	FY2018	FY2013
1 or 2	12%	5%
3 or 4	25%	21%
5 or 6	27%	29%
7 or 8	25%	30%
9 or 10	11%	15%
Total	100%	100%
Extrapolated value	5.46	6.08

Q3. What is the minimum educational requirement for job candidates? Please select all that apply.	FY2018	FY2013
One or more recognized professional certifications (such as CISSP)	52%	50%
On-the-job work experience (apprentice)	60%	53%
Certificate program specializing in IT security or directly related field	15%	14%
Associates degree specializing in IT security or directly related field	21%	19%
Bachelor's degree specializing in IT security or directly related field	39%	35%
Masters degree specializing in IT security or directly related field	16%	15%
None of the above	22%	24%
Total	225%	210%

Q4a. What general knowledge should an entry-level job candidate have? Please check all that apply.	FY2018
Understanding information security frameworks	18%
Familiarity with security regulations and standards	25%
Network and system administration experience	17%
Experience with intrusion prevention and detection systems	19%
Understanding of potential cybersecurity threats	39%
Knowledgeable about how to provide timely and relevant security reports	15%
Background in data loss prevention	9%
Understanding how to communicate to C-level executives and board members	5%
Other (please specify)	3%
Total	150%

Q4b. What general knowledge should a highly-experienced (at or above the supervisory level) job candidate have? Please check all that apply.	FY2018
Understanding information security frameworks	75%
Familiarity with security regulations and standards	73%
Network and system administration experience	63%
Experience with intrusion prevention and detection systems	81%
Understanding of potential cybersecurity threats	85%
Knowledgeable about how to provide timely and relevant security reports	63%
Background in data loss prevention	50%
Understanding how to communicate to C-level executives and board members	44%
Other (please specify)	5%
Total	539%

Q5a. What IT security technical skills should an entry-level job candidate have? Please check all that apply.	FY2018
Use big data analytics to pinpoint security threats	5%
Create, modify and update intrusion detection systems (IDS)	6%
Create, modify and update security information event management (SIEM) systems	5%
Discover vulnerabilities in information systems	16%
Evaluate and deconstruct malware software	21%
Monitor compliance with security regulations	10%
Install firewall and data encryption programs	16%
Maintain security records of monitoring and incident response activities	25%
Install firewall and data encryption programs	9%
Remediate security issues	8%
Respond to requests for specialized cyber threat reports	7%
Perform cyber and technical threat analyses	18%
Prevent hacker intrusion	13%
Produce situational and incident-related reports	6%
Other (please specify)	5%
Total	170%

Q5b. What IT security technical skills should a highly-experienced (at or above supervisory level) job candidate have? Please check all that apply.	FY2018
Use big data analytics to pinpoint security threats	33%
Create, modify and update intrusion detection systems (IDS)	55%
Create, modify and update security information event management (SIEM) systems	51%
Discover vulnerabilities in information systems	63%
Evaluate and deconstruct malware software	51%
Monitor compliance with security regulations	44%
Install firewall and data encryption programs	39%
Maintain security records of monitoring and incident response activities	49%
Install firewall and data encryption programs	42%
Remediate security issues	67%
Respond to requests for specialized cyber threat reports	70%
Perform cyber and technical threat analyses	74%
Prevent hacker intrusion	66%
Produce situational and incident-related reports	43%
Other (please specify)	41%
Total	788%

Part 3. The effect of automation on jobs in IT security

Q6. How will automation affect the hiring of IT security personnel? Please select only one response.	FY2018
Automation will increase the need to hire people with more advanced technical skills	44%
Automation will reduce the head count of our IT security function	23%
Automation will have no affect on our hiring and the head count of our IT security function	33%
Other (please specify)	0%
Total	100%

Q7. Does your organization use automation?	FY2018
Yes, currently	26%
No, but planning to in the next six to 12 months	46%
We do not plan to use automation (skip to Q11a)	28%
Total	100%

Q8. What activities currently performed by your IT security staff do you think automation will replace in the next three years? Please select all that apply.	FY2018
Threat intelligence	30%
Incident response	38%
Threat hunting	50%
Log analysis	65%
DevOps	32%
Responding to requests for cyber threat reports	29%
Other (please specify)	5%
None of the above	30%
Total	279%

Q9a. Do you personally think you will lose your job because of automation?	FY2018
Yes	25%
No	65%
Unsure	10%
Total	100%

Q9b. If yes, when do you think you will lose your job because of automation?	FY2018
Less than 1 year	12%
1 to 2 years	30%
3 to 4 years	29%
5 to 6 years	18%
7 to 10 years	5%
More than 10 year	6%
Total	100%
Extrapolated value	3.66

Q10a. Will automation improve your IT security staff's ability to do their jobs?	FY2018
Yes	60%
No	28%
Unsure	12%
Total	100%

Q10b. If yes, why?	FY2018
It will enable IT security staff to focus on more serious vulnerabilities and overall network security	68%
It will automate time intensive, manual processes that are mission critical but not a good use of staff time	44%
It will reduce human error	36%
Other (please specify)	7%
Total	155%

Q10c. If no, why?	FY2018
Automation will never replace human intuition and hands-on experience	55%
Automation will add complexity to jobs	46%
Automation is not able to catch certain threats	38%
Human intervention is necessary for network protection	51%
Automation is not capable of performing certain tasks that the IT security staff can do	67%
Other (please specify)	9%
Total	266%

Q11a. Is artificial intelligence (AI) a dependable and trusted security tool for your organization?	FY2018
Yes, at present	15%
Yes, within the next 12 to 24 months	23%
Yes, more than 24 months from now	33%
No	29%
Total	100%

Q11b. If yes, why?	FY2018
Human error is a major problem	34%
Our organization does not have sufficient manpower to monitor threats 24/7	44%
AI provides an additional layer of monitoring that we don't currently have in place	36%
AI is very helpful and it is a great addition to our other security tools	38%
Other (please specify)	4%
Total	156%

Q11c. If no, why?	FY2018
A machine cannot be trained to do the tasks performed by our security team (including myself)	56%
Our security team (including myself) is more qualified to catch threats and vulnerabilities in real-time	50%
Human intervention is necessary for network protection	45%
Other (please specify)	5%
Total	156%

Q12. In your organization, are IT security employees paid, on average, more than, less than or equal to other IT employees?	FY2018	FY2013
Paid more	53%	51%
Paid equally	39%	40%
Paid less	5%	5%
Unsure	3%	4%
Total	100%	100%

Q13a. Does your organization have a chief information security officer (CISO or equivalent title)?	FY2018	FY2013
Yes	53%	44%
No	47%	56%
Total	100%	100%

Q13b. If yes, does the CISO have final authority on whom to hire?	FY2018	FY2013
Yes	50%	49%
No	50%	51%
Total	100%	100%

Part 4. People skills

Q14. Using the following 10-point scale, please rate the importance of the ability to communicate technical information across all levels of the organization. .	FY2018
1 or 2	2%
3 or 4	11%
5 or 6	21%
7 or 8	24%
9 or 10	42%
Total	100%
Extrapolated value	7.36

Q15. Using the following 10-point scale, please rate the importance of being a team player.	FY2018
1 or 2	0%
3 or 4	9%
5 or 6	25%
7 or 8	30%
9 or 10	36%
Total	100%
Extrapolated value	7.36

Q16. Using the following 10-point scale, please rate the importance of creative problem solving.	FY2018
1 or 2	5%
3 or 4	6%
5 or 6	11%
7 or 8	37%
9 or 10	41%
Total	100%
Extrapolated value	7.56

Q17. Using the following 10-point scale, please rate the importance of having a good work ethic and being dependable.	FY2018
1 or 2	0%
3 or 4	0%
5 or 6	9%
7 or 8	41%
9 or 10	50%
Total	100%
Extrapolated value	8.32

Q18. Using the following 10-point scale, please rate the importance of being able to take direction and criticism well.	FY2018
1 or 2	4%
3 or 4	12%
5 or 6	19%
7 or 8	28%
9 or 10	37%
Total	100%
Extrapolated value	7.14

Q19. Using the following 10-point scale, please rate the importance of the ability to anticipate security incidents in advance.	FY2018
1 or 2	9%
3 or 4	15%
5 or 6	36%
7 or 8	22%
9 or 10	18%
Total	100%
Extrapolated value	6.00

Q20. Using the following 10-point scale, please rate the importance of having the necessary technical skills.	FY2018
1 or 2	0%
3 or 4	1%
5 or 6	19%
7 or 8	44%
9 or 10	36%
Total	100%
Extrapolated value	7.80

Q21a. How important are a job candidate's outside interests when hiring?	FY2018
Very important	25%
Important	28%
Somewhat important	22%
Not important	25%
Total	100%

Q21b. If important, what are the most desirable outside interests? Please check all that apply.	FY2018
Participating in team sports	53%
Working out on a regular basis	56%
Participating in the creative arts such as painting, music and creative writing	36%
Engaging in politics	12%
Traveling	37%
Learning other languages	52%
Volunteering and working with charities	60%
Other (please specify)	2%
Total	308%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	FY2018
Senior executive/VP	7%
Director	16%
Manager	21%
Supervisor	15%
Technician/staff/associate	41%
Total	100%

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	FY2018
CEO/executive committee	3%
Chief operating officer	0%
Chief information officer	40%
Chief information security officer	19%
Chief security officer	5%
Chief technology officer	7%
Chief financial officer	0%
Leader, human resources	0%
Leader, business unit or LOB	11%
Leader, corporate compliance	2%
Leader, risk management	8%
Leader, IT administration	2%
Data center management	3%
Total	100%

D3. What industry best describes your organization's primary sector?	FY2018
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	1%
Energy & utilities	5%
Financial services	18%
Health & pharmaceutical	11%
Hospitality & leisure	3%
Industrial & manufacturing	10%
Media & entertainment	3%
Public sector	9%
Retail	9%
Services	10%
Technology & software	8%
Transportation	2%
Other	2%
Total	100%

D4. What is the worldwide head count of your organization?	FY2018
Less than 1,000	14%
1,000 to 5,000	26%
5,001 to 10,000	23%
10,001 to 25,000	18%
25,001 to 75,000	11%
More than 75,00	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.

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.