Staffing the IT Security Function in the Age of Automation: A Study of Organizations in the United States, United Kingdom and APAC

Ponemon Institute© Research Report

Staffing the IT Security Function in the Age of Automation: A Study of Organizations in the United States, United Kingdom and APAC

Prepared by Ponemon Institute, April 2019

Part 1. Introduction

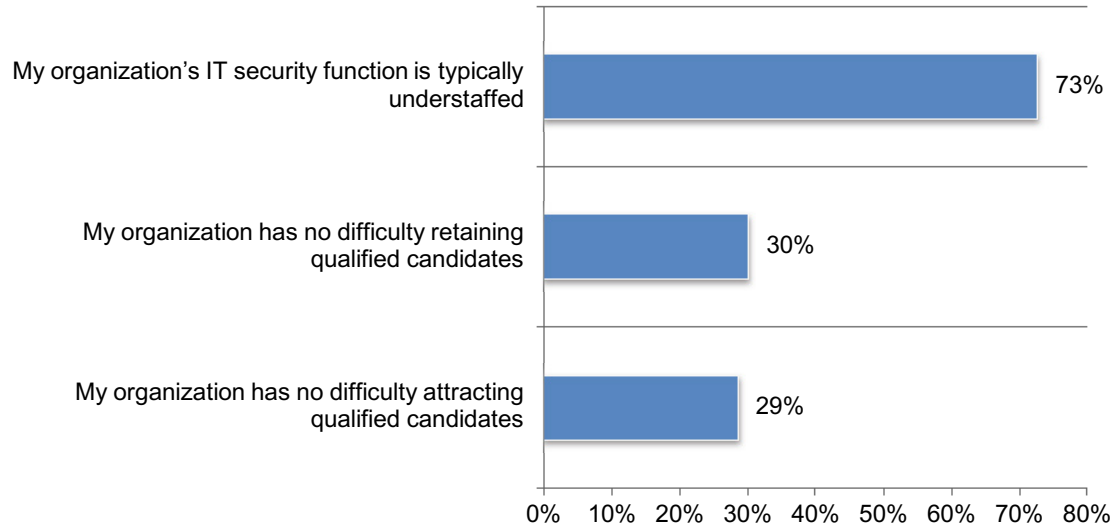
Organizations globally are facing a shortage of IT security staff. Ponemon Institute, with sponsorship from DomainTools, conducted the study *Staffing the IT Security Function in the Age of Automation* to better understand how organizations are addressing the problem of attracting and retaining IT security practitioners and how the adoption of automation and artificial intelligence (AI) will impact IT security.

More than 1,400 IT and IT security practitioners in the US, UK and APAC who participate in attracting, hiring, promoting and retaining IT security personnel within their organizations were surveyed. Most of the respondents are IT directors, managers and IT systems analysts. According to these participants their IT security teams can be overwhelmed with security incidents they must respond to.

Figure 1 reveals that 73 percent of respondents believe their organization's IT security functions are typically understaffed due to the difficulty in attracting and retaining qualified candidates. Only 29 percent of respondents say they have **no difficulty** attracting and only 30 percent of respondents say they have **no difficulty** retaining qualified candidates.

Figure 1. Why organizations' IT functions are understaffed

Strongly agree and Agree responses combined



The key takeaway from the following findings is that the use of automation will not reduce the headcount in the IT security function. Instead, according to respondents, automation will mean increased job security for IT security practitioners, especially those who have the expertise to manage these technologies.

- Sixty-five percent say human involvement in security is important in the age of automation.
- A barrier to adopting automation is the lack of in-house expertise, according to 56 percent of respondents.

- Automation improves the ability to prioritize threats and vulnerabilities (49 percent of respondents) and increases the productivity of current security personnel (47 percent of respondents).

- Headcount of the IT security function is not likely to be reduced. Automation will either have no effect on hiring (25 percent of respondents) or will increase hiring (40 percent of respondents).

- Most respondents (61 percent) do not think they will lose their jobs because of automation.

- Automation will enable IT security staff to focus on more serious vulnerabilities and overall network security (68 percent of respondents).

- Sixty-five percent of respondents say automation is not capable of performing certain tasks that IT security staff can do, and 51 percent of respondents say automation will never replace human intuition and hands-on experience.

- Artificial intelligence is supportive of organizations' efforts to monitor threats. Sixty-three percent of respondents say their organization does not have enough staff to monitor threats on a 24/7 basis.

Part 2. Key findings

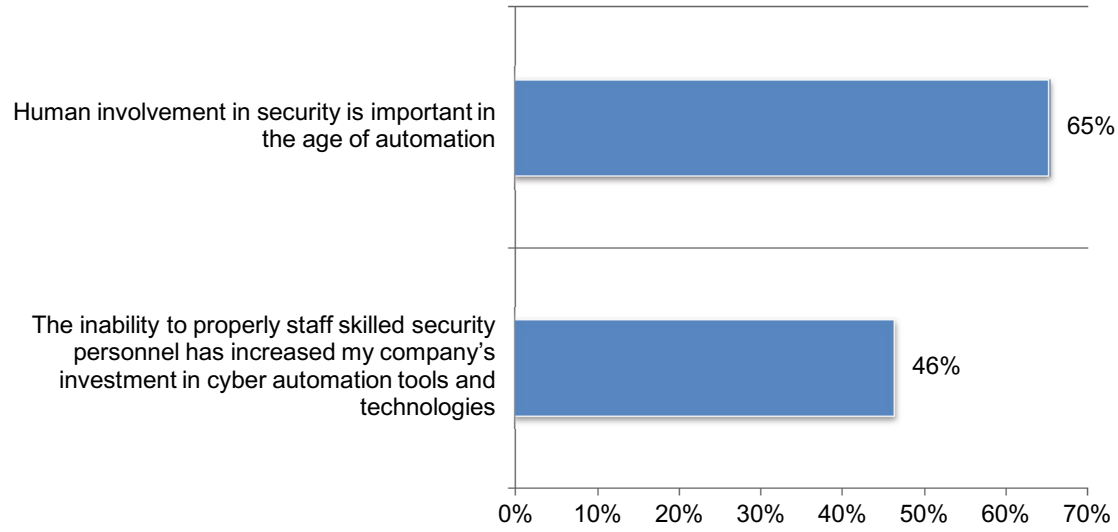
This section presents a detailed analysis of the research. The complete audited findings are presented in the Appendix of this report, which is organized according to the following topics:

- How automation influences the staffing of the IT security function
- The effect of automation, artificial intelligence and other technologies on the IT security team
- Technical skills and general knowledge in demand
- Country and regional differences

How automation influences the staffing of the IT security function

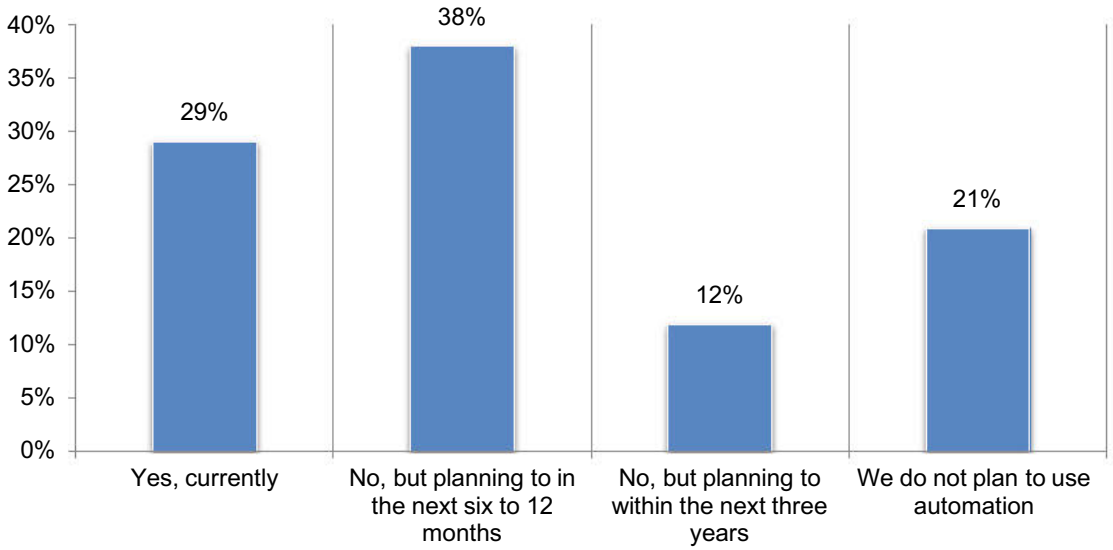
Automation will not replace human involvement in IT security. As shown in Figure 2, less than half of respondents (46 percent) say the inability to properly staff their IT functions with skilled personnel has resulted in an increase in the investment in cyber automation tools and technologies. Sixty-five percent of respondents think human involvement is important when using automation.

Figure 2. Perceptions about cyber automation and the IT security function
Strongly agree and Agree responses combined



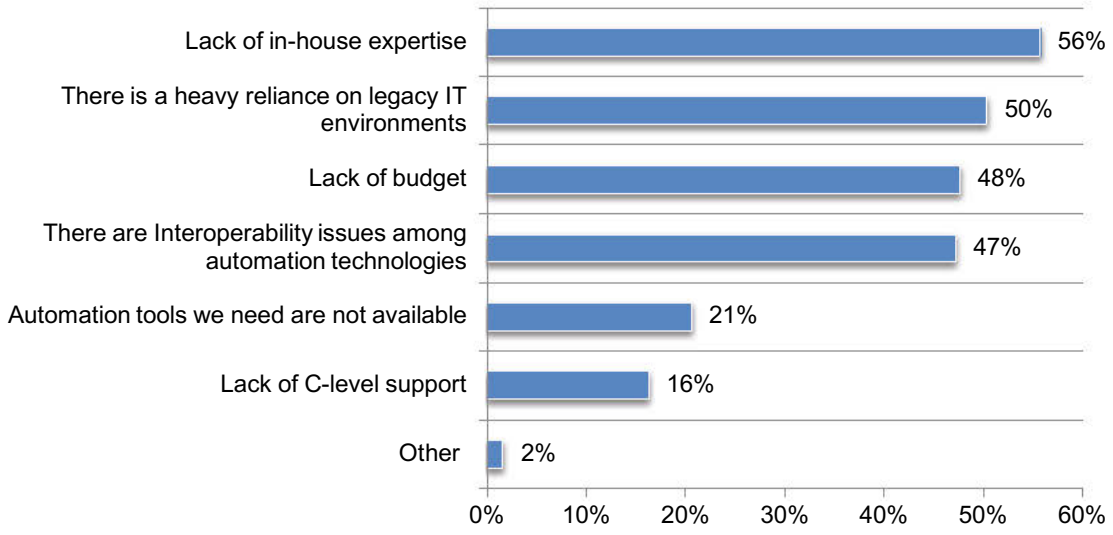
Most organizations are investing in automation. As shown in Figure 3, 79 percent of respondents either use automation currently or plan to in the future. However, as discussed above, these investments are not likely to replace skilled IT security practitioners.

Figure 3. Does your organization use automation?



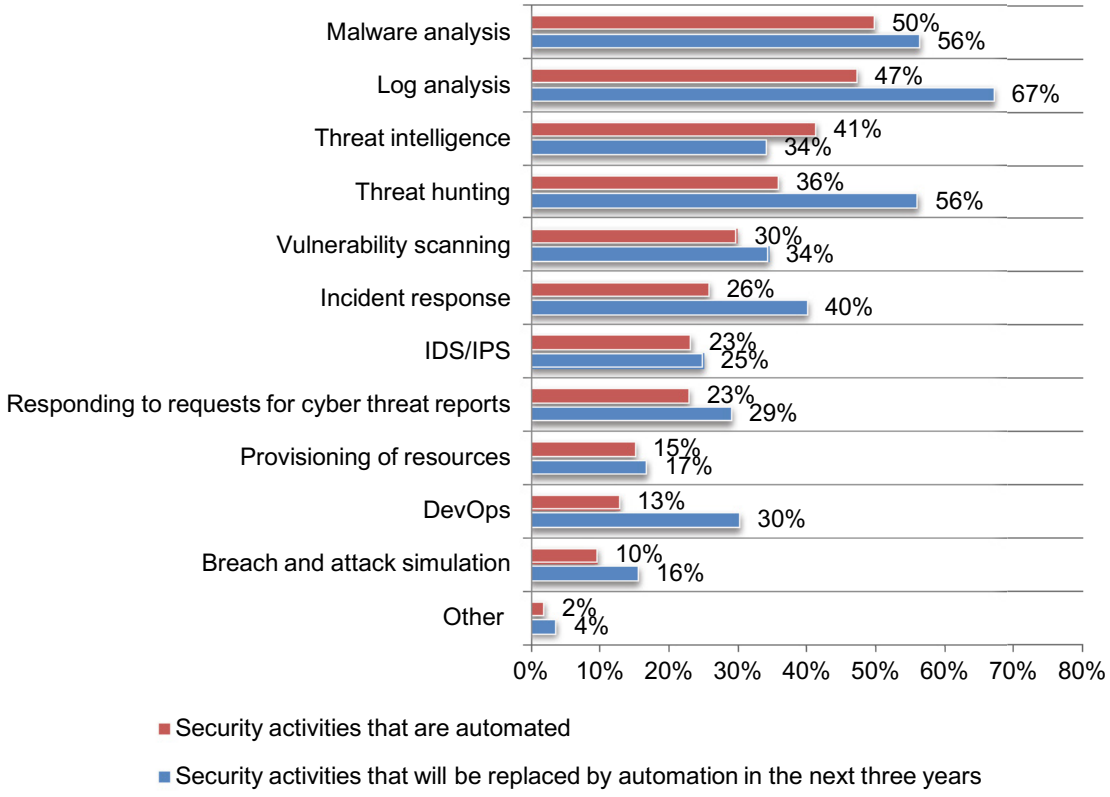
A barrier to adopting automation is the lack of in-house expertise. As Figure 4 shows, of the 21 percent of respondents who have no plan to adopt automation in their organizations, 56 percent say their choice is due to not having the necessary skilled IT security practitioners to manage these solutions. A further 50 percent say they do not plan to adopt automation because their organizations rely heavily upon legacy IT environments.

Figure 4. Reasons why organizations do not adopt automation
More than one response permitted



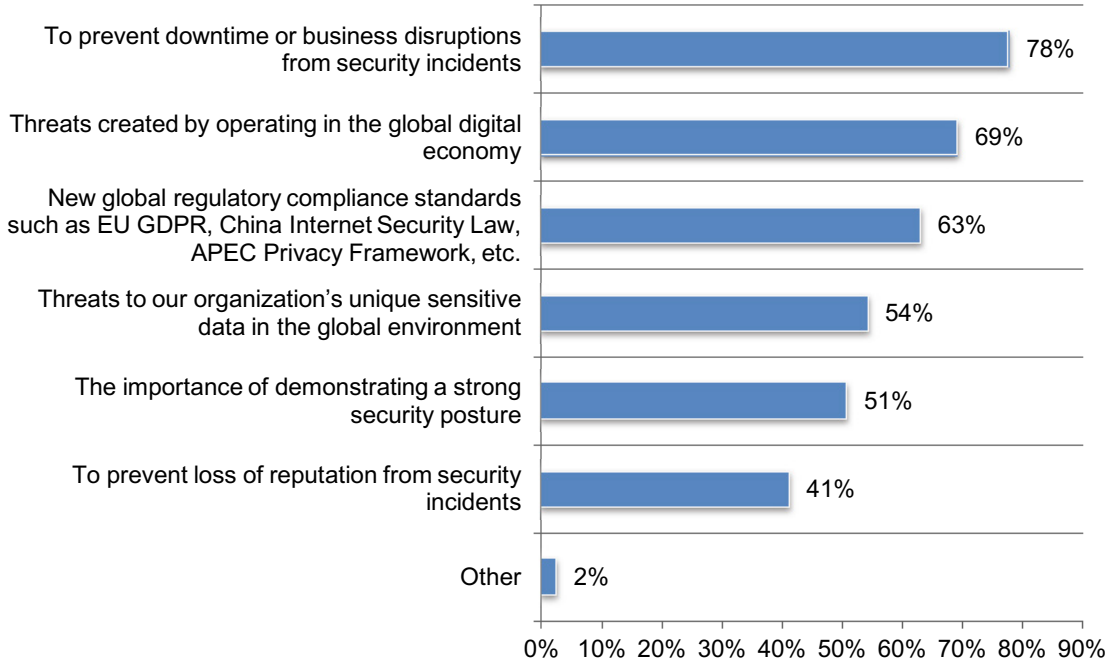
Automation is relieving IT security teams of malware and log analysis. As reported previously, 79 percent of respondents say their organizations currently use or plan to use automation within the next three years. The most likely tasks that are or will be automated are malware analysis, log analysis and threat intelligence, as shown in Figure 5

Figure 5. What security activities are most commonly automated or will be automated in the next three years?
More than one response permitted



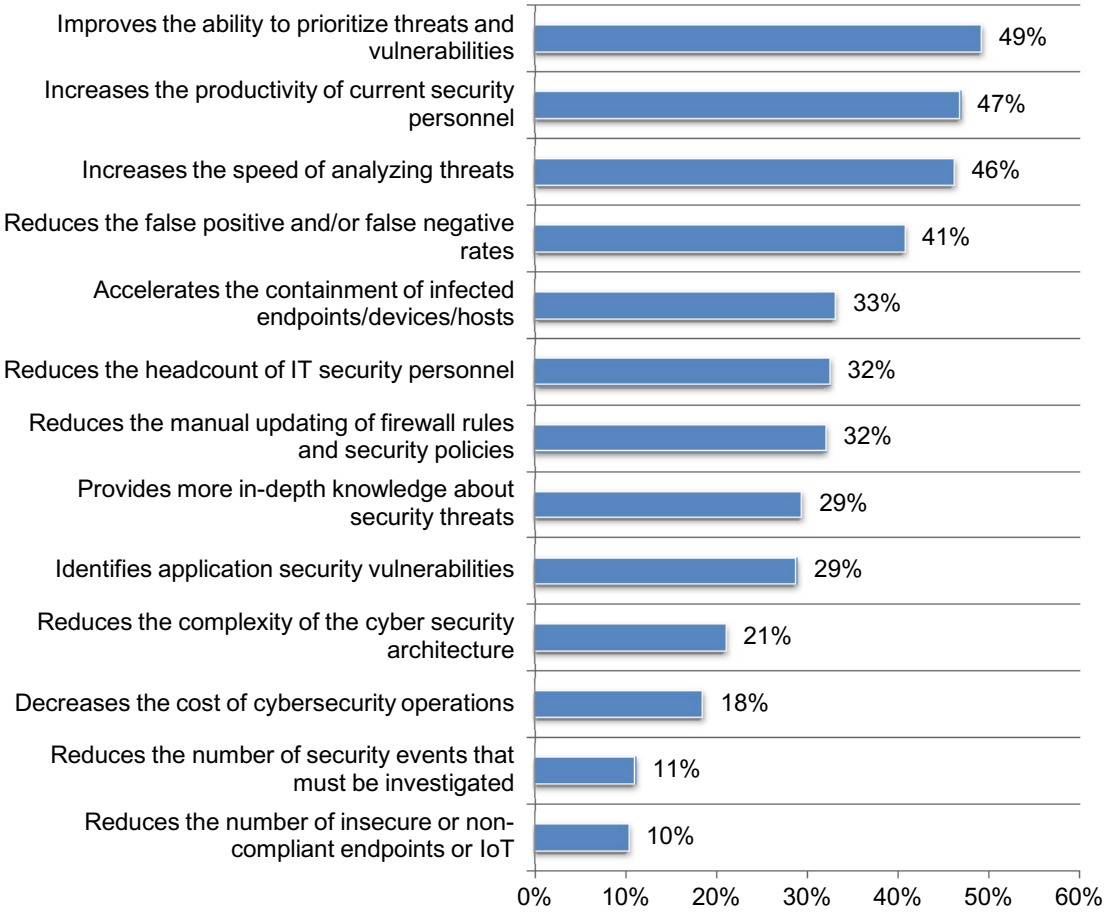
Global business and security factors have a major influence on the adoption of automation. The majority of respondents believe that most of the factors listed in Figure 6 do affect the decision to invest in automation. The two top reasons are preventing downtime or business disruptions caused by security incidents (78 percent of respondents) and threats created by operating in the global digital economy (69 percent of respondents).

Figure 6. What global business and security factors influence adoption of automation
More than one response permitted



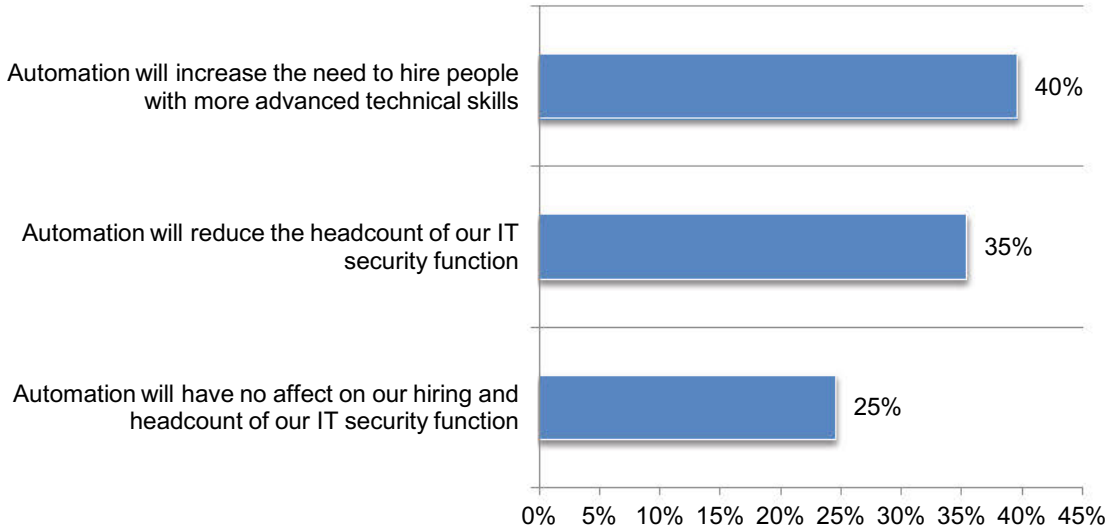
Automation increases the productivity of security personnel. The productivity and effectiveness of IT security staff is increased because automation improves the ability to prioritize threats and vulnerabilities and increases the speed of analysis. However, few respondents say it decreases the cost of cybersecurity operations, reduces the number of security events that must be investigated and the number of insecure or non-compliant endpoints or IoT devices.

Figure 7. What are the primary benefits of automation?
More than one response permitted



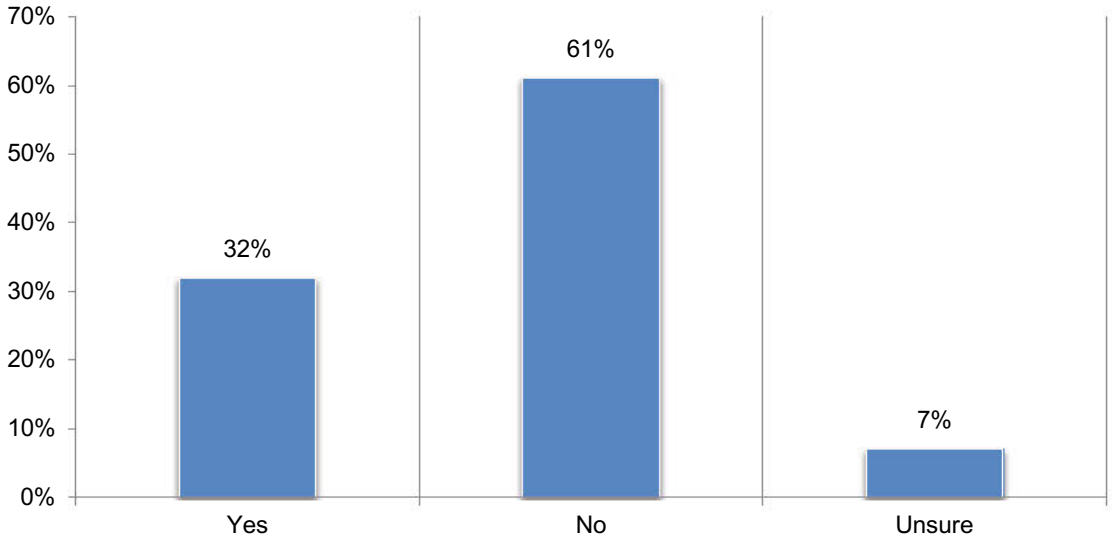
Automation will not reduce the need for IT security professionals. As shown in Figure 8, 65 percent of respondents predict automation will either increase the need to hire people with more advanced skills (40 percent) or it will not affect the headcount of their IT security function (25 percent). Only 35 percent of respondents say automation will reduce the number of professionals employed in their IT security function.

Figure 8. How will automation affect the hiring of IT security personnel?



Most respondents are confident they will not lose their job because of automation. According to Figure 9, 61 percent of respondents do not think they will lose their jobs as a result of automation. Of the 32 percent who say they are concerned about keeping their job, the majority believe this will happen in an average of 3 years.

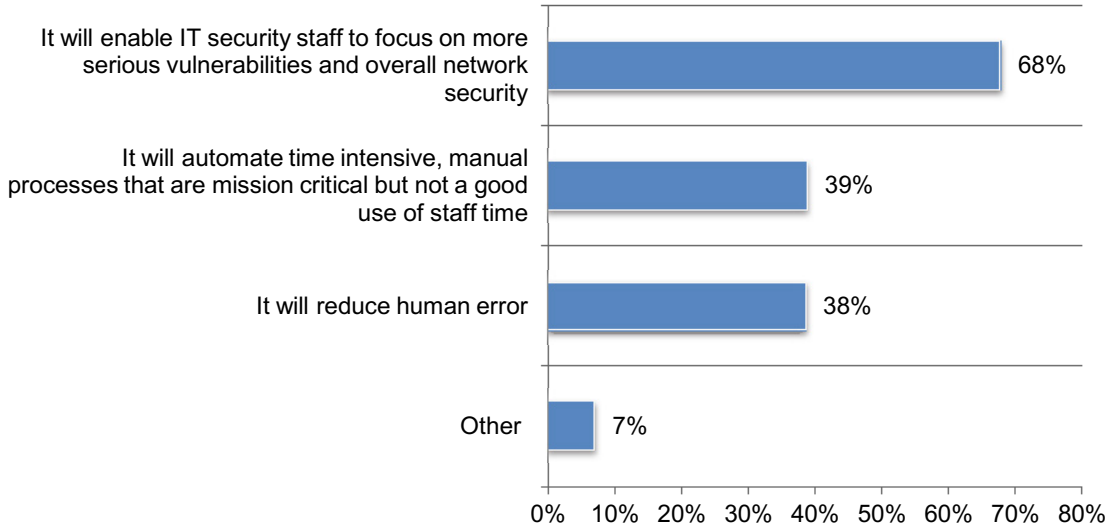
Figure 9. Do you personally think you will lose your job because of automation?



The effect of automation, artificial intelligence and other technologies on the IT security team

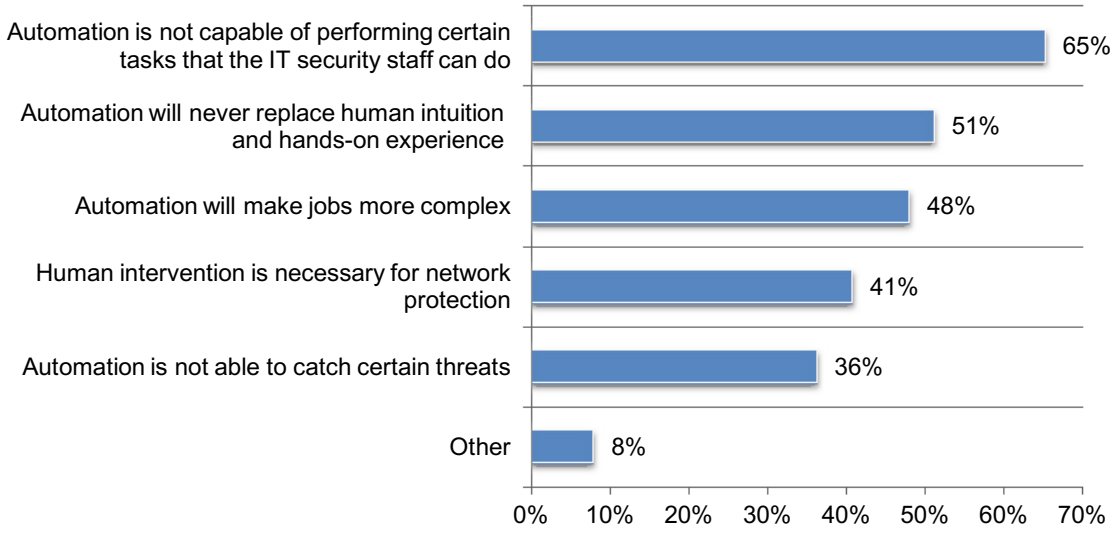
Automation is expected to make IT security staff more effective in creating a stronger security posture. According to Figure 10, 68 percent of respondents think automation will enable IT security staff to focus on more serious vulnerabilities and overall network security. Moreover, 39 percent of respondents think that automation will also be able to relieve staff of lengthy, manual processes that are mission critical but not very time and cost effective.

Figure 10. How will automation improve the ability of their IT security staff to do their jobs?
More than one response permitted



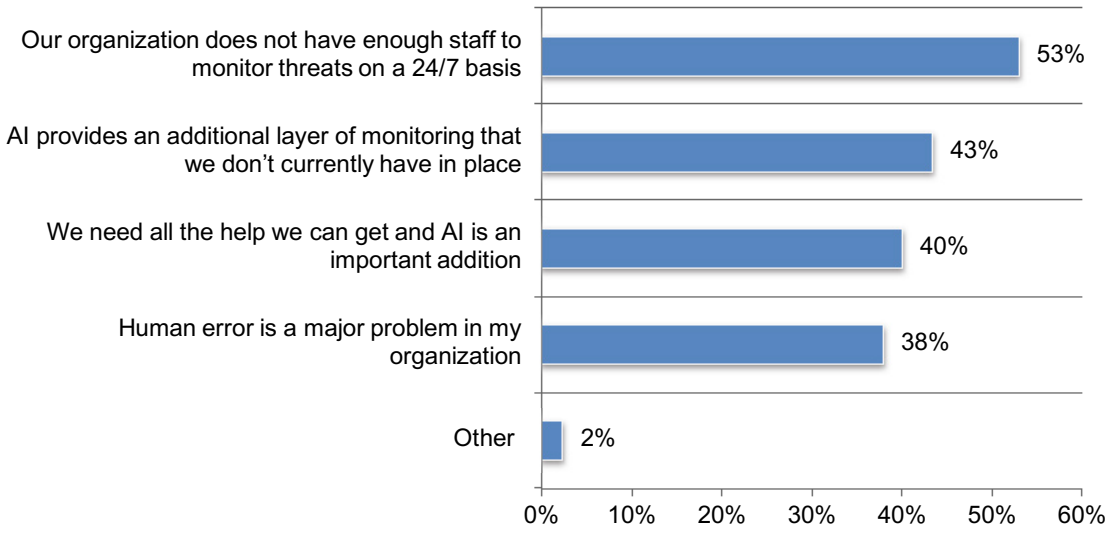
There are more reasons why automation will not replace IT security staff. As shown in Figure 11, a good proportion of respondents think that their jobs within the IT security function will be safe even as their organization adopts automation. Sixty-five percent of respondents say automation is not capable of performing certain tasks that IT security staff can do, while 51 percent of respondents maintain that it will never replace human intuition and hands-on experience.

Figure 11. How will automation *not* improve your IT security staff's ability to do their job?
More than one response permitted



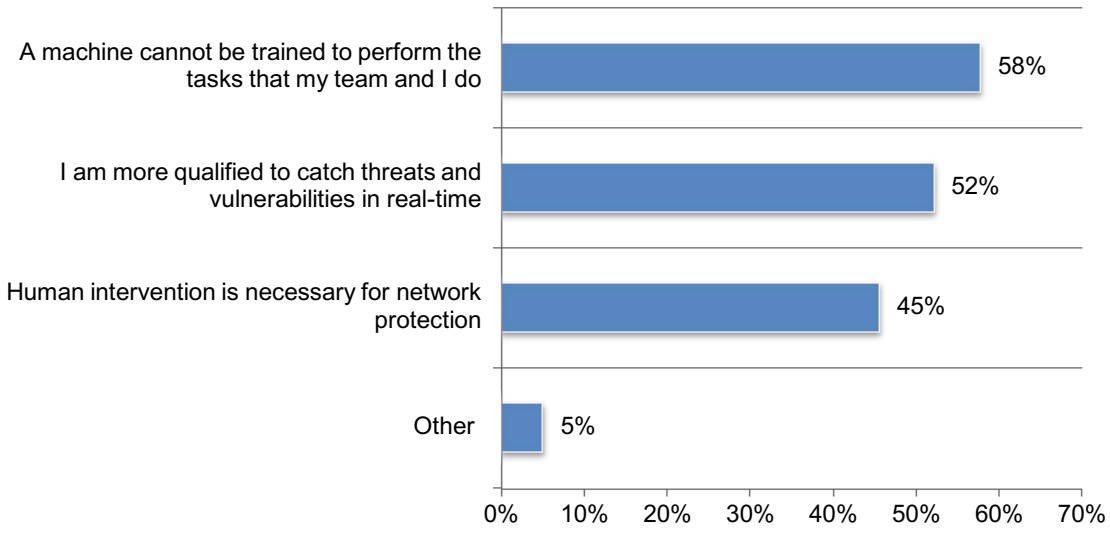
AI is supportive of an organization's efforts to monitor threats. Seventy percent of respondents say AI is a trusted part of their security solutions. As shown in Figure 12, the primary reason is the lack of in-house resources to monitor threats continuously. Fifty-three percent of respondents say their organizations do not have enough staff to monitor threats on a 24/7 basis. Forty-three percent of respondents say AI provides an additional layer of monitoring that they don't currently have in place.

Figure 12. Why is AI a dependable and trusted security tool?
More than one response permitted



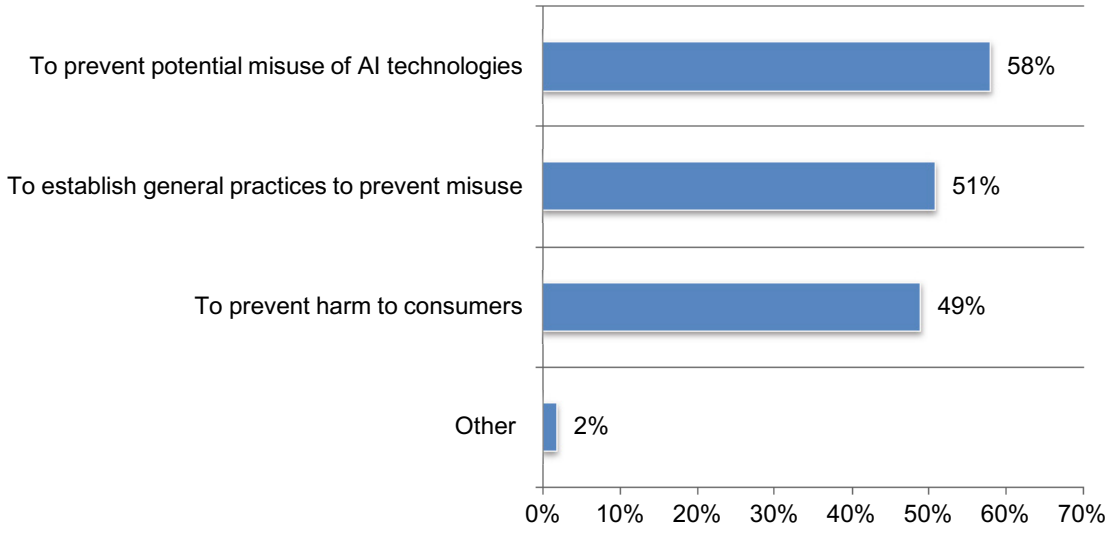
According to the 30 percent of respondents who say AI is not a trusted part of their organizations' security arsenal, the primary reason is that a machine cannot be trained to perform the tasks their team does (58 percent of respondents), while 52 percent of respondents say they are more qualified to catch threats and vulnerabilities in real time, as shown in Figure 13.

Figure 13. Why AI is not considered dependable and trusted
More than one response permitted



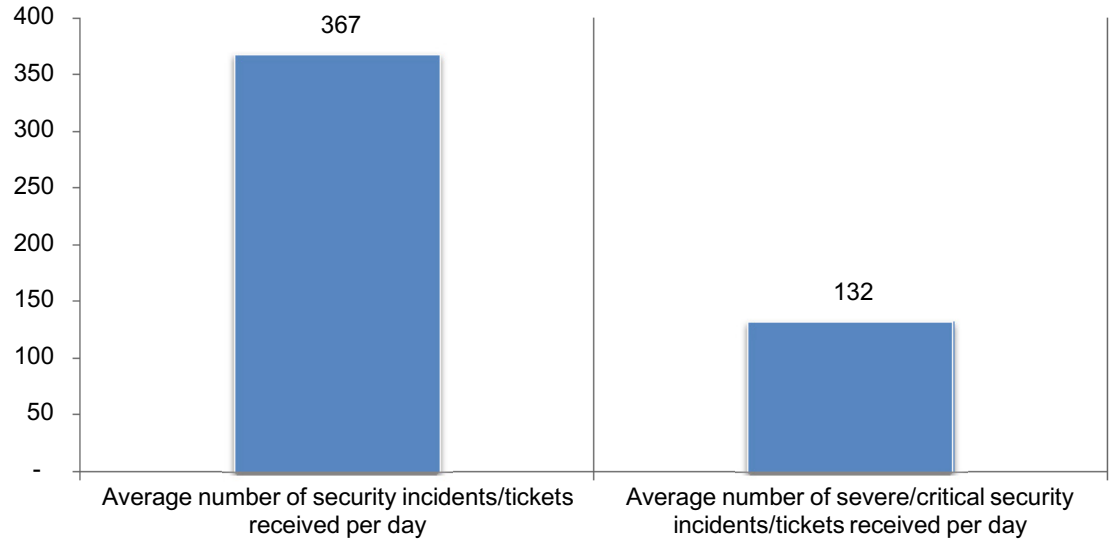
Should the use of AI be regulated? Respondents were asked if the government should regulate organizations' use of AI and 25 percent of respondents agree that it should be. Reasons for regulation are shown in Figure 14. The two top reasons are to prevent potential misuse of AI technologies and to establish general practices to prevent misuse, with 58 percent and 51 percent of respondents, respectively.

Figure 14. Why government should regulate AI
More than one response permitted



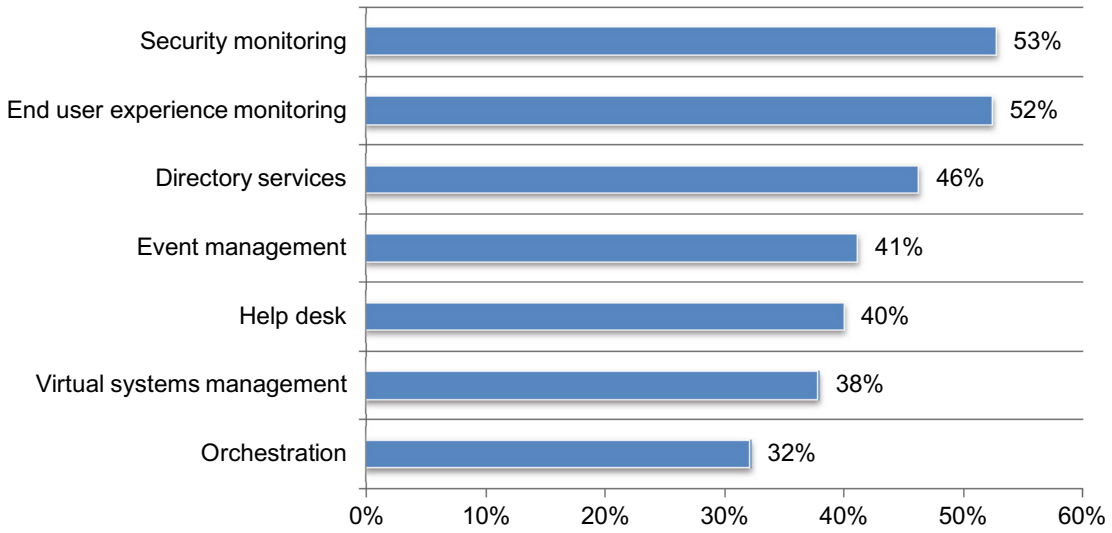
As shown in Figure 15, security teams receive an average of almost 500 security incidents/tickets (367) and severe/critical security incidents (132) per day. The typical security team spends an average of 55 staff hours investigating or triaging alerts each day.

Figure 15. The average number of security and severe security incidents/tickets the security team receives each day
Extrapolated values presented



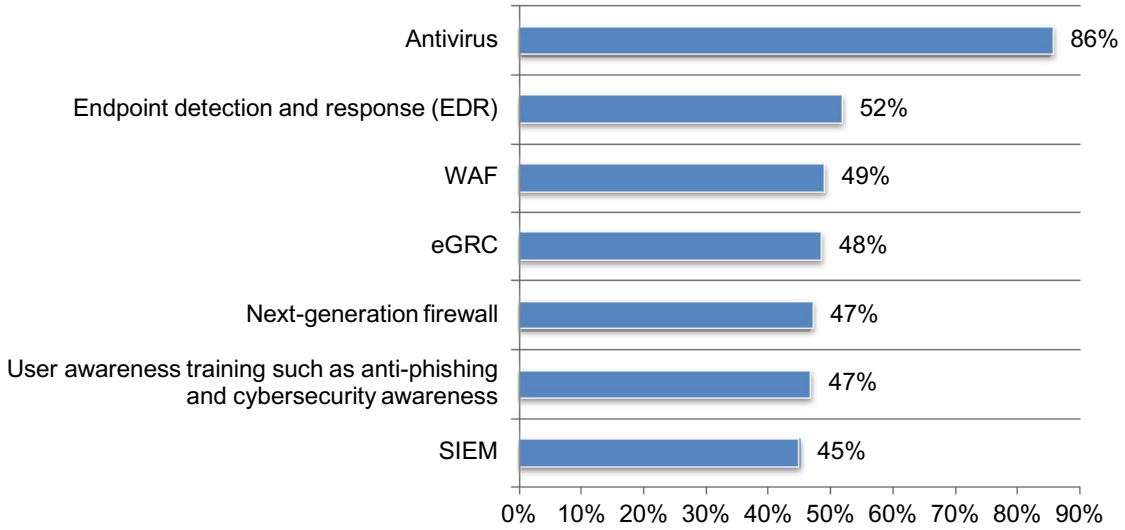
Monitoring technologies are the solutions most often integrated with organizations' security management tools. Security monitoring and end-user experience monitoring are in the top 7 of solutions integrated in security management tools. They are followed by directory services and event management, as Figure 16 shows.

Figure 16. The top 7 solutions integrated with organizations' security management tools
More than one response permitted



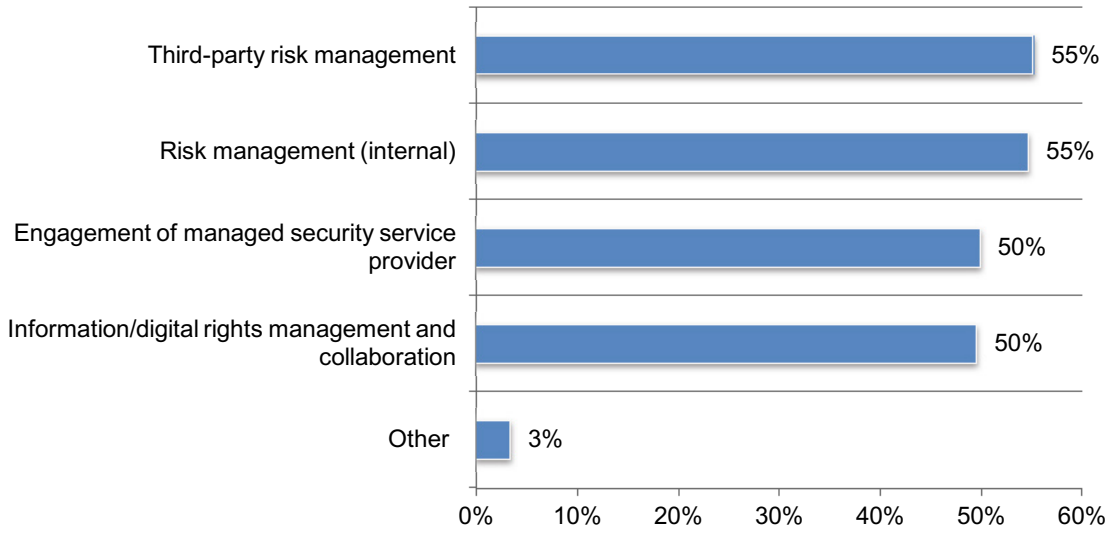
As shown in Figure 17, the top two security technology solutions used in organizations are antivirus and endpoint detection and response (EDR).

Figure 17. The top 7 security technology solutions deployed today
More than one response permitted



Organizations are most concerned about risks created by their third-party suppliers and partners. As highlighted in Figure 18, 55 percent of respondents say their governance practices address third party risks, and another 55 percent of respondents say they have procedures in place to manage internal risks.

Figure 18. Governance practices organizations implement
More than one response permitted



Technical skills and general knowledge in demand

An understanding of potential cybersecurity threats is important for both entry-level and highly experienced job candidates. As shown in Figure 19, highly experienced job candidates are expected to be knowledgeable about a wide range of governance and technology issues. These include an understanding of potential cybersecurity threats, experience with intrusion prevention and detection systems, and familiarity with security regulations and standards.

Figure 19. What knowledge should entry-level and highly experienced job candidates have?
More than one response permitted

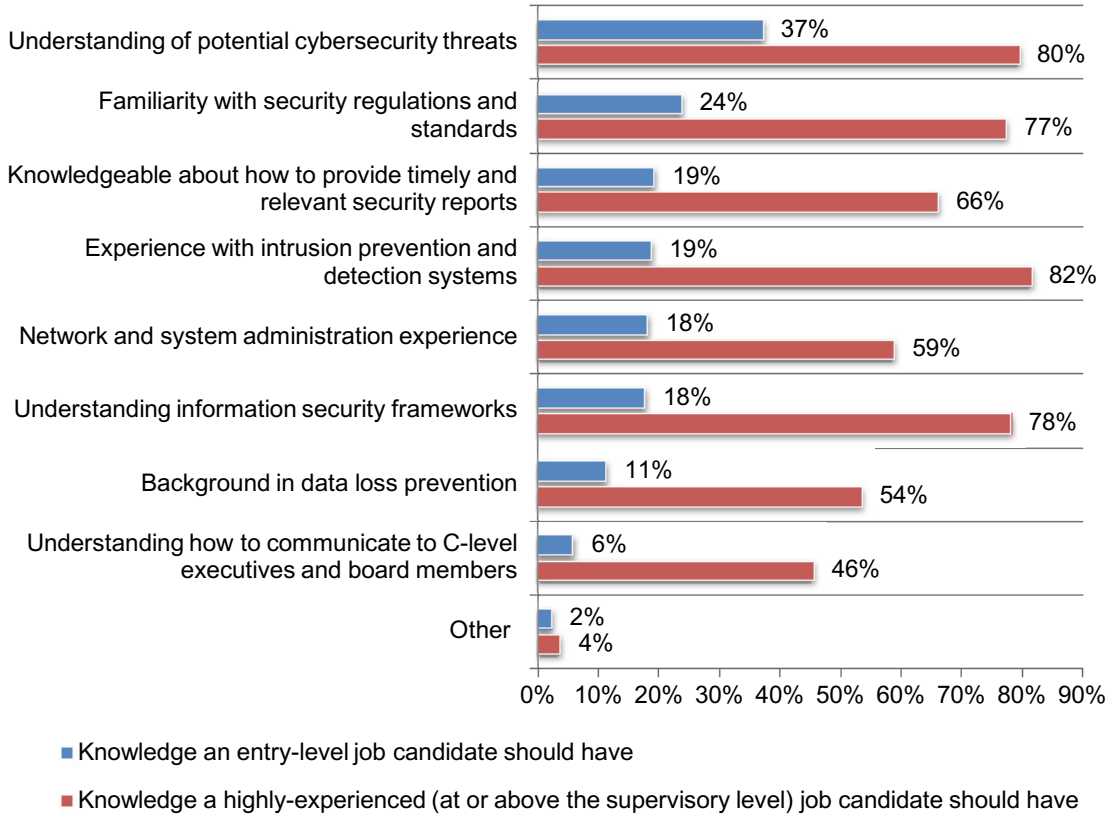
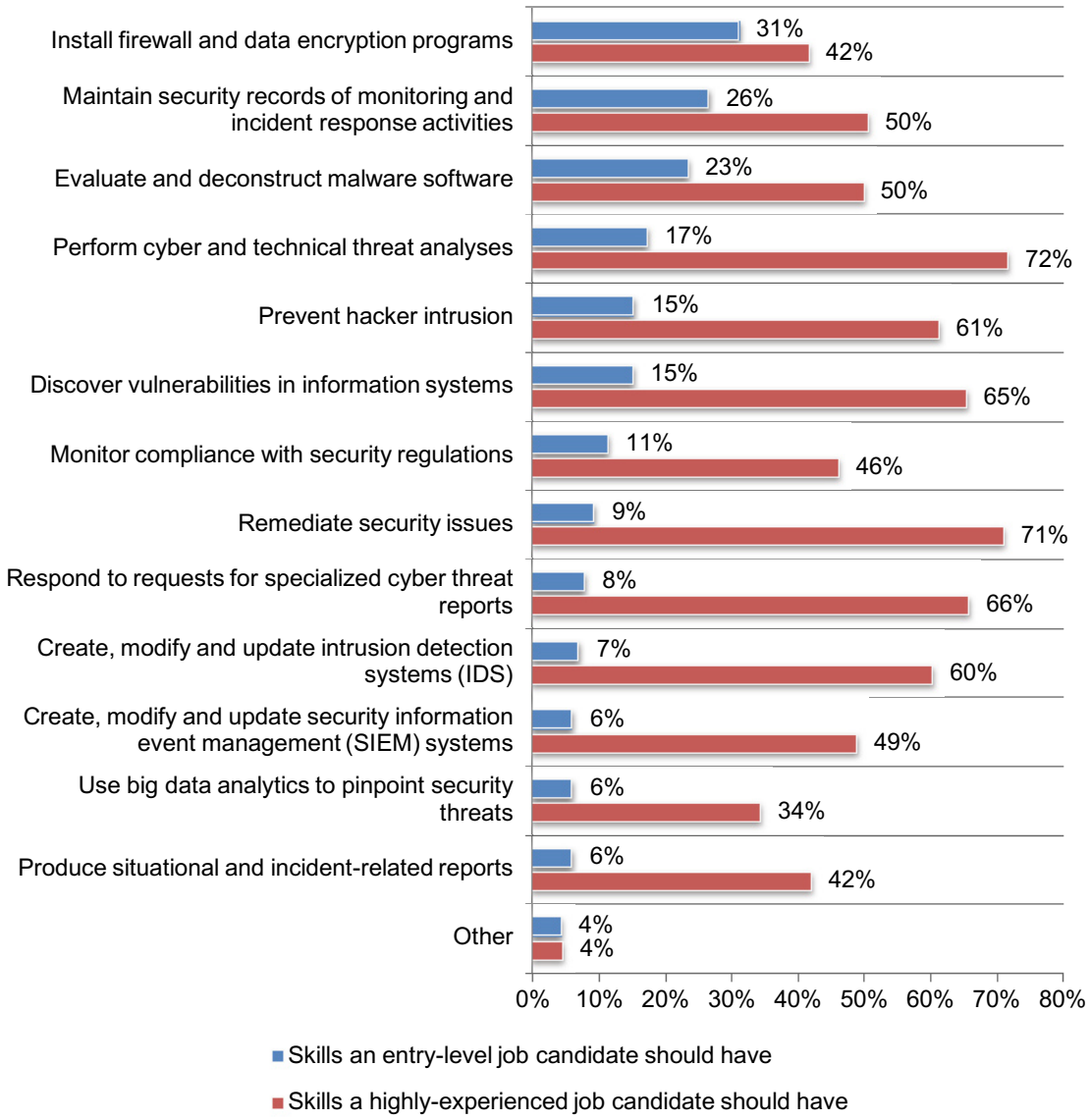


Figure 20 shows that entry-level job candidates are expected to have more tactical technical skills, such as installing firewall and data encryption programs and maintain security records of monitoring and incident response activities. Highly experienced job candidates, on the other hand, are mostly expected to have the skills to perform cyber and technical threat analyses, remediate security issues, and respond to requests for specialized cyber threat reports.

Figure 20. What IT security technical skills should entry-level and highly experienced job candidates have?
More than one response permitted

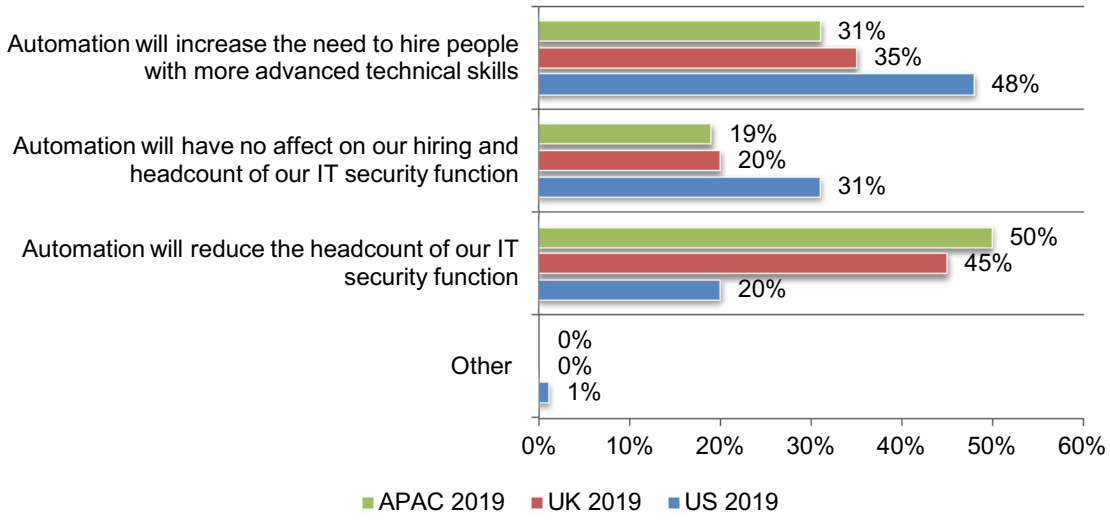


Country and regional differences

In this section, we present the most salient differences among APAC[1] (403 respondents), the UK (402 respondents) and the US (633 respondents). The key takeaway in this analysis is that US respondents are the most positive about the ability of automation and AI to make IT security staff more productive while not reducing the need to hire experienced practitioners.

Will automation affect headcount? According to Figure 21**,** respondents in the US are far more positive than the UK and APAC that automation will increase the need to hire expert IT security practitioners and least likely to believe it will reduce headcount. In fact, 50 percent of respondents in APAC say their IT security teams will become smaller because of automation.

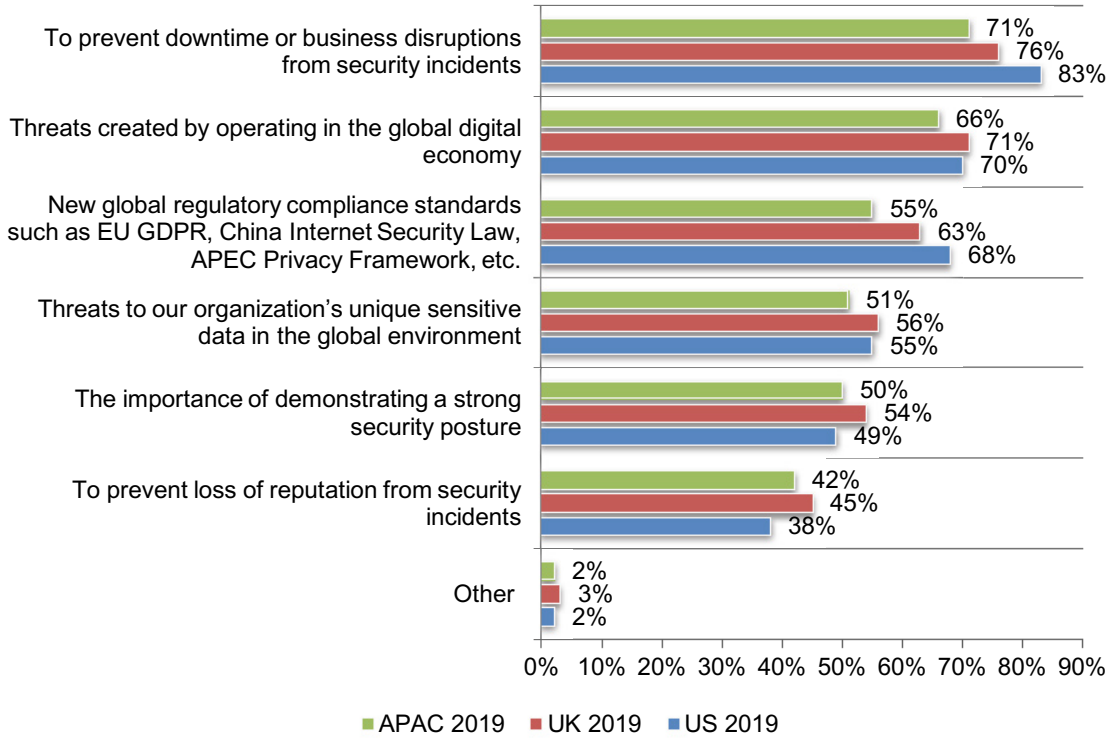
Figure 21. How will automation affect the hiring of IT security personnel?



[1] Countries in the APAC cluster include Australia, China (PRC), India, Indonesia, Japan, Korea, New Zealand, Philippines, Singapore, Taiwan, Thailand and Vietnam

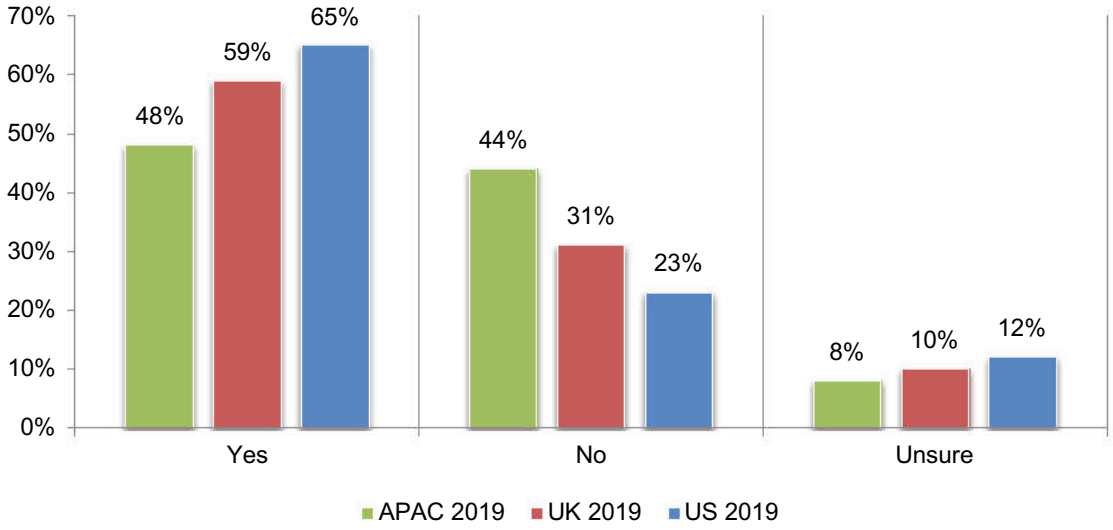
Prevention of downtime from security incidents is a global concern. As shown in Figure 22, the US, UK and APAC all agree that the two factors that are most likely to drive the adoption of automation are prevention of downtime or business disruptions from security incidents and threats created by operating in the global economy. Respondents in the US are most likely to adopt automation because of global regulations.

Figure 22. Factors in the global business and security landscape that influence the adoption of automation
More than one response permitted



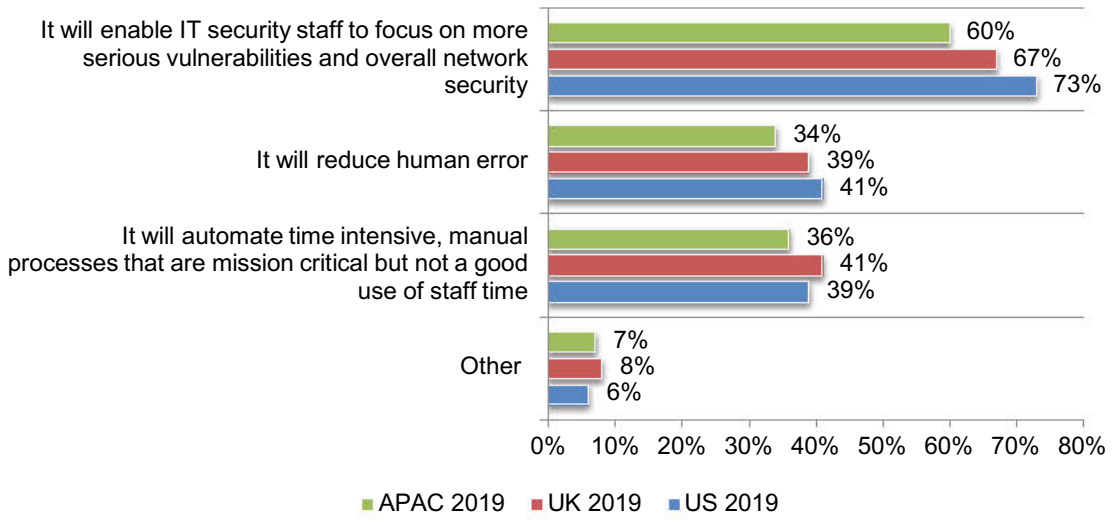
APAC respondents are far less likely to believe automation improves the IT security staff's ability to do their work. US respondents are more likely to be positive about the benefits of automation in making the IT security staff more efficient and productive, as shown in Figure 23.

Figure 23. Will automation improve your IT security staff's ability to do their jobs?



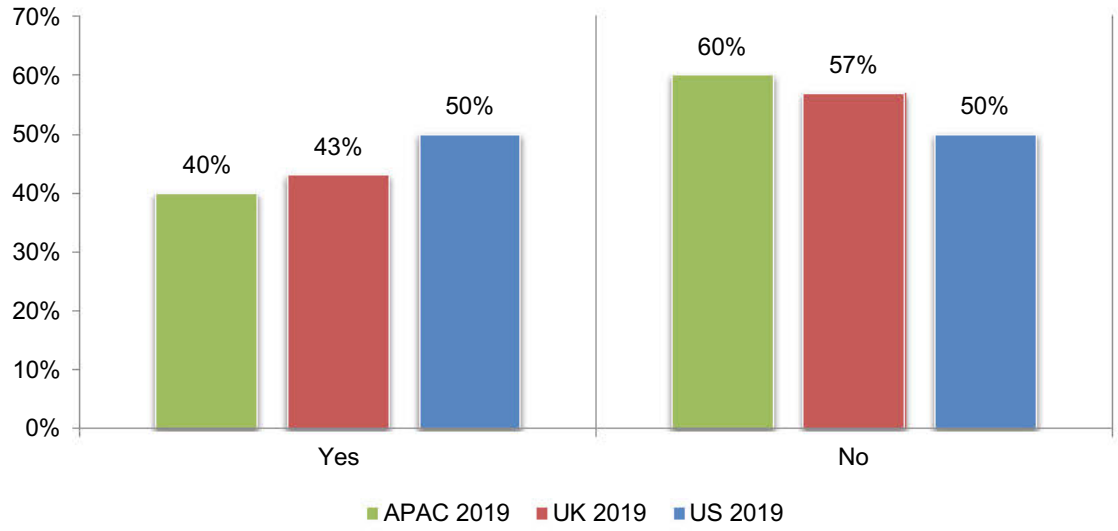
According to Figure 24, if automation is believed to improve the effectiveness of the IT security team, the main reason is that it will enable them to focus on more serious vulnerabilities and overall network security.

Figure 24. Why automation will improve the IT security staff's ability to do their jobs?
More than one response permitted



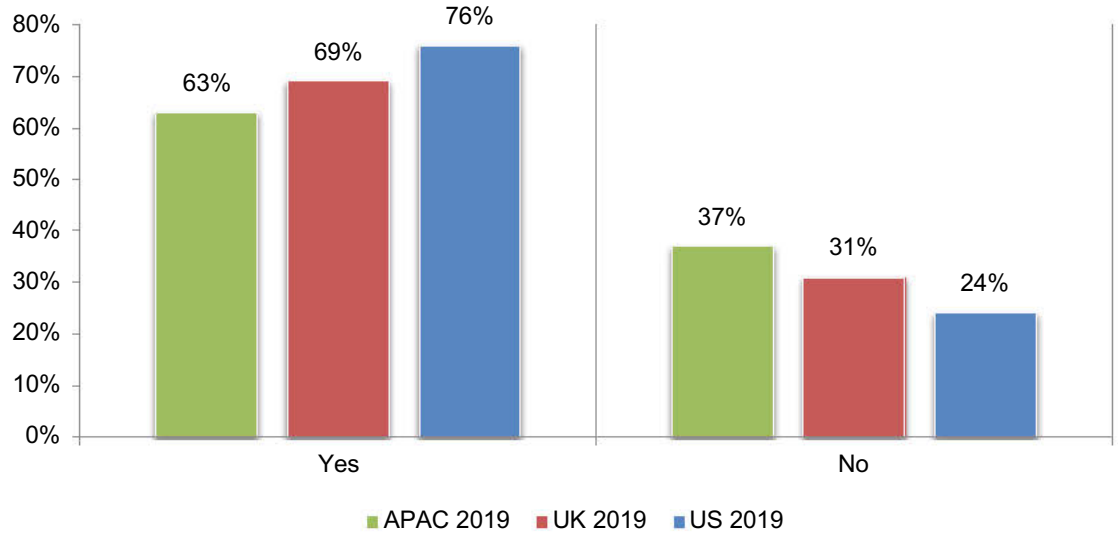
US respondents are also most likely to believe attackers are increasing their use of automation (50 percent of respondents) versus 40 percent of respondents in APAC as shown in Figure 25.

Figure 25. Do you see an increase in attackers' use of automation?



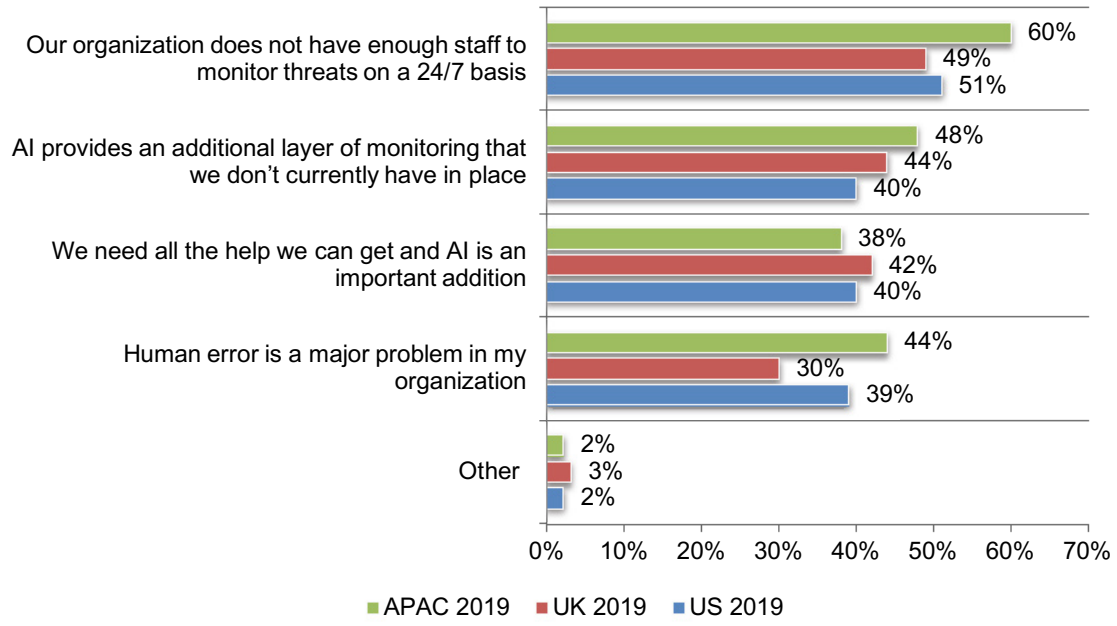
There are interesting differences in the trust of AI as a security tool. According to Figure 26, 76 percent of US respondents versus 63 percent of APAC respondents say they trust AI as a security tool in their organizations.

Figure 26. Do you trust AI as a security tool in your organization?



AI is trusted because it enhances organizations' ability to monitor threats. As shown in Figure 27, 60 percent of APAC respondents say their organizations are understaffed and therefore unable to monitor threats on a 24/7 basis. Forty-eight percent of these respondents also believe AI provides an additional layer of monitoring that they don't currently have in place.

Figure 27. Why do you trust AI as a security tool in your organization?
More than one response permitted



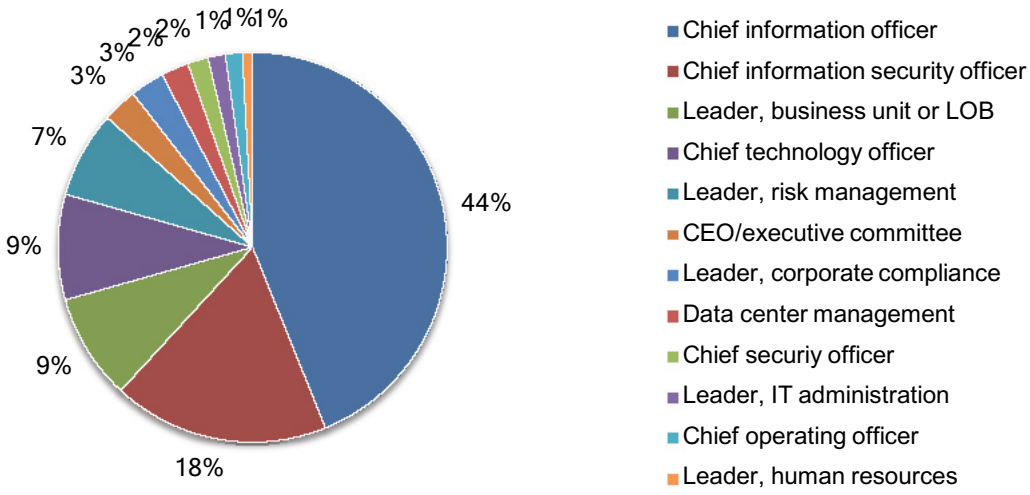
Part 3. Methods

A sampling frame of 38,948 IT and IT security practitioners located in the US, the UK and APAC, and who participate in attracting, hiring, promoting and retaining IT security personnel in their organizations were selected as participants in this survey. Table 1 shows 1,593 total returns. Screening and reliability checks required the removal of 155 surveys. Our final sample consisted of 1,438 surveys, or a 3.7 percent response rate. Respondents have been at their current position for an average of six years and have an average of 9 years of relevant experience.

Table 1. Sample response	FY2019	Pct%
Sampling frame	38,948	100%
Total returns	1,593	4.1%
Rejected or screened surveys	155	0.4%
Final sample	1,438	3.7%

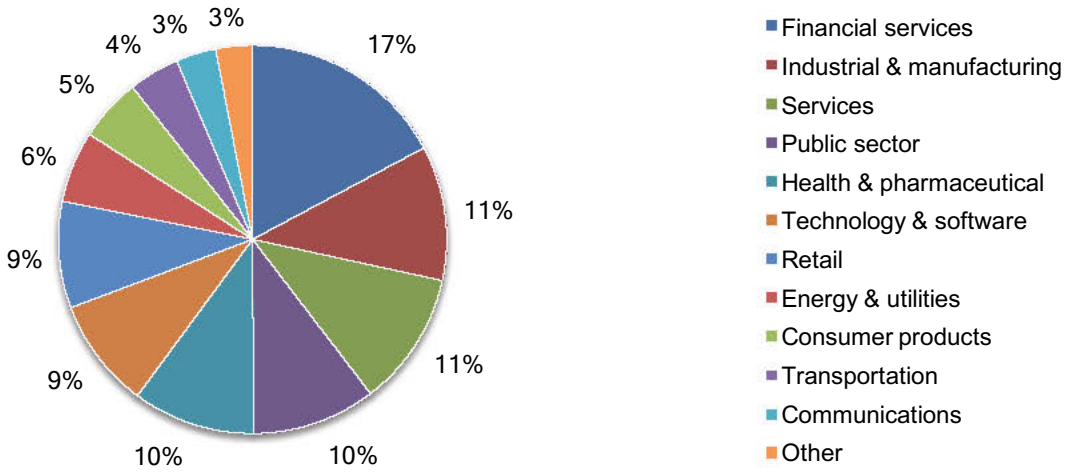
As shown in Pie Chart 1, 44 percent of respondents report to the chief information officer, 18 percent of respondents report to the chief information security officer, 9 percent of respondents report to the business unit leader and 9 percent of respondents indicated they report to the chief technology officer.

Pie Chart 1. Primary person you or your leader reports to



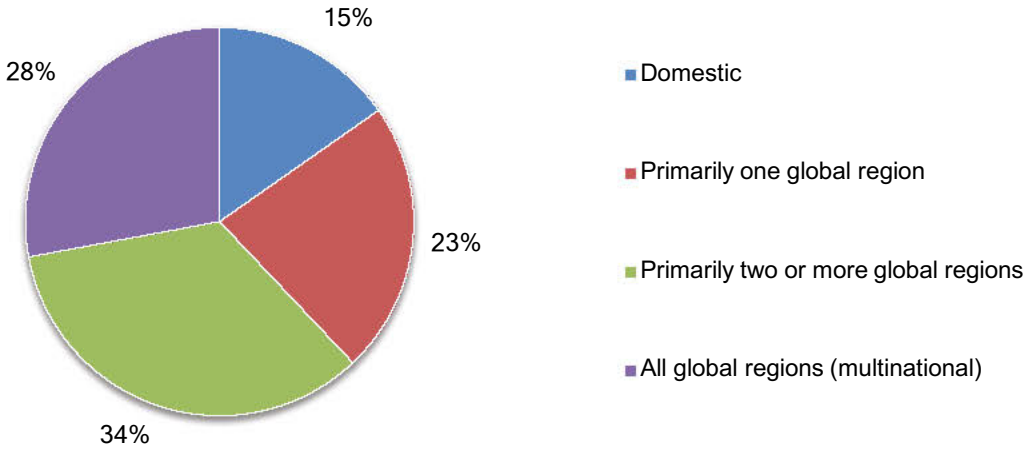
Pie Chart 2 reports the industry segments of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by industrial and manufacturing (11 percent of respondents), services sector (11 percent of respondents), public sector (10 percent of respondents) and health and pharmaceuticals (10 percent of respondents).

Pie Chart 2. Industry distribution of respondents' organizations



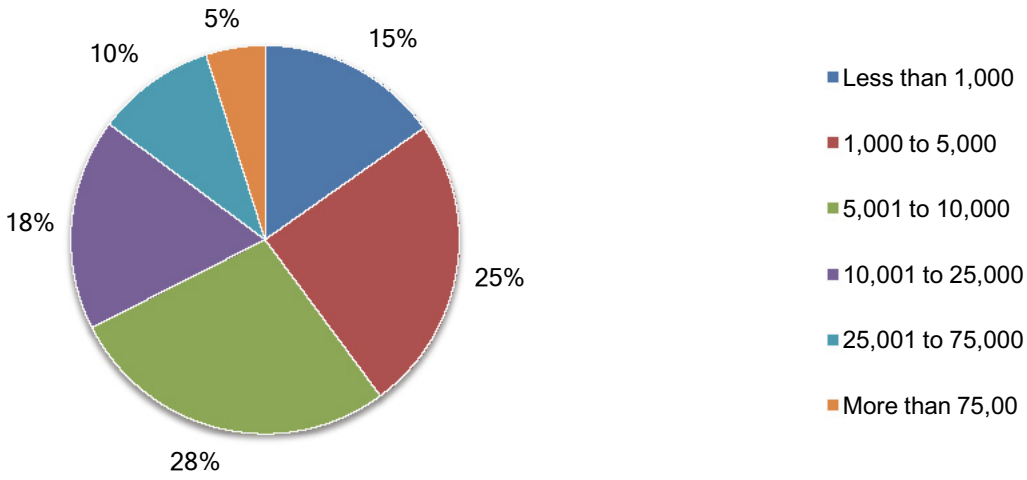
Pie Chart 3 reports the geographic footprint of the respondents' organizations. Thirty-four percent of respondents are from organizations with a geographic footprint of primarily two or more global regions, 28 percent of respondents are from multinational organizations, 23 percent are from organizations with primarily one global region and 15 percent of respondents are from domestic organizations.

Pie Chart 3. Distribution of respondents' organizations by geographic footprint



Pie Chart 4 reports the worldwide headcount of the respondents' organizations. More than half of respondents (61 percent) are from organizations with a worldwide headcount greater than 5,000 employees.

Pie Chart 4. Worldwide headcount 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 2019.

Survey response	APAC 2019	UK 2019	US 2019	Total
Total sampling frame	11,507	10,988	16,453	38,948
Total returns	450	445	698	1,593
Rejected surveys	47	43	65	155
Final sample	403	402	633	1,438
Response rate	3.5%	3.7%	3.8%	3.7%

Part 1. Screening Questions

S1. What best describes your role/title in the organization? Please select only **one** choice.	Total
Chief information officer (CIO)	5%
Chief information security officer (CISO)	7%
Chief risk officer (CRO)	3%
Chief security officer (CSO)	3%
Chief technology officer (CTO)	2%
Infrastructure engineer (security/systems)	1%
IT administrator	2%
IT architect	2%
IT business analyst	1%
IT consultant/Integrator	3%
IT director	12%
IT manager	11%
IT project/program manager	4%
IT security operations staff	9%
IT software engineer/developer	9%
IT systems analyst/programmer/engineer	10%
IT vice president	2%
Line of business director	3%
Line of business manager/supervisor	4%
Line of business staff	5%
Line of business vice president/general manager	2%
None of the above (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**	Total
Q1a. My organization has no difficulty **attracting** qualified candidates.	29%
Q1b. My organization has no difficulty **retaining** qualified candidates.	30%
Q1c. My organization's IT security function is typically understaffed.	73%
Q1d. My company's use of cyber automation will reduce its need for skilled IT security personnel.	30%
Q1e. The inability to properly staff skilled security personnel has increased my company's investment in cyber automation tools and technologies.	46%
Q1f. Human involvement in security is important in the age of automation.	65%

Q2a. What knowledge should an entry-level job candidate have? Please select all that apply.	Total
Background in data loss prevention	11%
Experience with intrusion prevention and detection systems	19%
Familiarity with security regulations and standards	24%
Knowledgeable about how to provide timely and relevant security reports	19%
Network and system administration experience	18%
Understanding how to communicate to C-level executives and board members	6%
Understanding information security frameworks	18%
Understanding of potential cybersecurity threats	37%
Other (please specify)	2%
Total	154%

Q2b. What knowledge should a highly-experienced (at or above the supervisory level) job candidate have? Please select all that apply..	Total
Background in data loss prevention	54%
Experience with intrusion prevention and detection systems	82%
Familiarity with security regulations and standards	77%
Knowledgeable about how to provide timely and relevant security reports	66%
Network and system administration experience	59%
Understanding how to communicate to C-level executives and board members	46%
Understanding information security frameworks	78%
Understanding of potential cybersecurity threats	80%
Other (please specify)	4%
Total	545%

Q3a. What IT security technical skills should an entry-level job candidate have? Please select all that apply.	Total
Create, modify and update intrusion detection systems (IDS)	7%
Create, modify and update security information event management (SIEM) systems	6%
Discover vulnerabilities in information systems	15%
Evaluate and deconstruct malware software	23%
Install firewall and data encryption programs	31%
Maintain security records of monitoring and incident response activities	26%
Monitor compliance with security regulations	11%
Perform cyber and technical threat analyses	17%
Prevent hacker intrusion	15%
Produce situational and incident-related reports	6%
Remediate security issues	9%
Respond to requests for specialized cyber threat reports	8%
Use big data analytics to pinpoint security threats	6%
Other (please specify)	4%
Total	185%

Q3b. What IT security technical skills should a highly-experienced (at or above supervisory level) job candidate have? Please select all that apply.	Total
Create, modify and update intrusion detection systems (IDS)	60%
Create, modify and update security information event management (SIEM) systems	49%
Discover vulnerabilities in information systems	65%
Evaluate and deconstruct malware software	50%
Install firewall and data encryption programs	42%
Maintain security records of monitoring and incident response activities	50%
Monitor compliance with security regulations	46%
Perform cyber and technical threat analyses	72%
Prevent hacker intrusion	61%
Produce situational and incident-related reports	42%
Remediate security issues	71%
Respond to requests for specialized cyber threat reports	66%
Use big data analytics to pinpoint security threats	34%
Other (please specify)	4%
Total	713%

Q4a. Does your organization invest in training/onboarding security personnel?	Total
Yes	52%
No	48%
Total	100%

Q4b. If yes, how many days does the training/onboarding take?	Total
Less than 1 day	38%
1 day	28%
2 to 3 days	18%
4 to 5 days	9%
1 week	4%
More than 1 week	2%
Total	100%
Extrapolated value	1.84

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

Q5a. Does your organization use automation?	Total
Yes, currently	29%
No, but planning to in the next six to 12 months	38%
No, but planning to within the next three years	12%
We do not plan to use automation	21%
Total	100%

Q5b. If no, why are you not adopting automation? Please select all that apply.	Total
Automation tools we need are not available	21%
There is a heavy reliance on legacy IT environments	50%
There are Interoperability issues among automation technologies	47%
Lack of budget	48%
Lack of in-house expertise	56%
Lack of C-level support	16%
Other (please specify)	2%
Total	239%

Q6. If yes, what percentage of IT security tasks have been automated?	Total
1% to 10%	11%
11% to 25%	38%
26% to 50%	36%
51% to 75%	13%
76% to 100%	2%
Total	100%
Extrapolated value	31%

Q7. What security activities are most commonly automated? Please select all that apply.	Total
Breach and attack simulation	10%
DevOps	13%
IDS/IPS	23%
Incident response	26%
Log analysis	47%
Malware analysis	50%
Provisioning of resources	15%
Responding to requests for cyber threat reports	23%
Threat hunting	36%
Threat intelligence	41%
Vulnerability scanning	30%
Other (please specify)	2%
Total	315%

Q8. What are the primary benefits of automation? Please select your top four choices.	Total
Accelerates the containment of infected endpoints/devices/hosts	33%
Decreases the cost of cybersecurity operations	18%
Identifies application security vulnerabilities	29%
Improves the ability to prioritize threats and vulnerabilities	49%
Increases the productivity of current security personnel	47%
Increases the speed of analyzing threats	46%
Provides more in-depth knowledge about security threats	29%
Reduces the complexity of the cyber security architecture	21%
Reduces the false positive and/or false negative rates	41%
Reduces the headcount of IT security personnel	32%
Reduces the manual updating of firewall rules and security policies	32%
Reduces the number of insecure or non-compliant endpoints or IoT	10%
Reduces the number of security events that must be investigated	11%
Other (please specify)	1%
Total	400%

Q9. What factors in the global business and security landscape influence your organization's adoption of automation? Please select all that apply.	Total
New global regulatory compliance standards such as EU GDPR, China Internet Security Law, APEC Privacy Framework, etc.	63%
Threats to our organization's unique sensitive data in the global environment	54%
Threats created by operating in the global digital economy	69%
The importance of demonstrating a strong security posture	51%
To prevent downtime or business disruptions from security incidents	78%
To prevent loss of reputation from security incidents	41%
Other (please specify)	2%
Total	358%

Q10. How will automation affect the hiring of IT security personnel? Please select only one choice.	Total
Automation will increase the need to hire people with more advanced technical skills	40%
Automation will reduce the headcount of our IT security function	35%
Automation will have no affect on our hiring and headcount of our IT security function	25%
Other (please specify)	0%
Total	100%

Q11a. Do you personally think you will lose your job because of automation?	Total
Yes	32%
No	61%
Unsure	7%
Total	100%

Q11b. If yes, when do you think you will lose your job because of automation?	Total
Less than 1 year	13%
1 to 2 years	32%
3 to 4 years	29%
5 to 6 years	16%
7 to 10 years	7%
More than 10 years	2%
Total	100%
Extrapolated value	3.31

Q12. 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.	Total
Breach and attack simulation	16%
DevOps	30%
IDS/IPS	25%
Incident response	40%
Log analysis	67%
Malware analysis	56%
Provisioning of resources	17%
Responding to requests for cyber threat reports	29%
Threat hunting	56%
Threat intelligence	34%
Vulnerability scanning	34%
Other (please specify)	4%
Total	408%

Q13a. Will automation improve your IT security staff's ability to do their jobs?	Total
Yes	59%
No	31%
Unsure	10%
Total	100%

Q13b. If yes, why? Please select all that apply.	Total
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	39%
It will reduce human error	38%
Other (please specify)	7%
Total	152%

Q13c. If no, why? Please select all that apply.	Total
Automation will never replace human intuition and hands-on experience	51%
Automation will make jobs more complex	48%
Automation is not able to catch certain threats	36%
Human intervention is necessary for network protection	41%
Automation is not capable of performing certain tasks that the IT security staff can do	65%
Other (please specify)	8%
Total	249%

Q14a. Do you trust artificial intelligence as a security tool in your organization? *responses different in FY2018	Total
Yes	70%
No	30%
Total	100%

Q14b. If no, why? Please select all that apply.	Total
A machine cannot be trained to perform the tasks that my team and I do	58%
I am more qualified to catch threats and vulnerabilities in real-time	52%
Human intervention is necessary for network protection	45%
Other (please specify)	5%
Total	160%

Q14c. If yes, why? Please select all that apply.	Total
Human error is a major problem in my organization	38%
Our organization does not have enough staff to monitor threats on a 24/7 basis	53%
AI provides an additional layer of monitoring that we don't currently have in place	43%
We need all the help we can get and AI is an important addition	40%
Other (please specify)	2%
Total	176%

Q15. Do you see an increase in attackers' use of automation?	Total
Yes	45%
No	55%
Total	100%

Q16a. Should government regulate organizations' use of artificial intelligence (AI)?	Total
Yes	25%
No	68%
Unsure	8%
Total	100%

Q16b. If yes, why should the use of AI be regulated? Please select all that apply.	Total
To prevent potential misuse of AI technologies	58%
To prevent harm to consumers	49%
To establish general practices to prevent misuse	51%
Other (Please specify)	2%
Total	159%

Part 4. Technical security questions

Q17. Does your organization have a security operations center (SOC)?	Total
Yes	55%
No	45%
Total	100%

Q18. On average, how many security incidents/tickets does the security team receive **per day**?	Total
Less than 25	3%
26 to 50	9%
51 to 100	18%
101 to 250	24%
251 to 500	24%
501 to 1,000	13%
More than 1,000	10%
Total	100%
Extrapolated value	367

Q19. On average, how many severe/critical security incidents/tickets does the security team receive **per day**?	Total
Less than 25	13%
26 to 50	27%
51 to 100	30%
101 to 250	20%
251 to 500	5%
501 to 1,000	4%
More than 1,000	1%
Total	100%
Extrapolated value	132

Q20. Approximately how many staff hours does your organization spend investigating or triaging alerts **per day**?	Total
1 to 5	4%
6 to 10	7%
11 to 25	14%
26 to 50	29%
51 to 100	32%
More than 100	13%
Total	100%
Extrapolated value	55

Q21. Which of the following does your organization require to be integrated with its security management tools? Please select all that apply.	Total
Advanced IT analytics	19%
Application dependency mapping	14%
Application performance management	14%
Change management	31%
Cloud services analytics	17%
CMDP	24%
Cross-domain operations	22%
Directory services	46%
End user experience monitoring	52%
Event management	41%
Help desk	40%
Orchestration	32%
Security monitoring	53%
Virtual systems management	38%
Other (please specify)	1%
Total	444%

Q22. Today, which of the following security technology solutions does your organization deploy? Please select all that apply.	Total
Advanced breach detection	38%
Advanced security/threat analytics and anomaly detection	44%
Advanced testing attack simulation	26%
Antivirus	86%
Cloud application security management	38%
eGRC	48%
Endpoint detection and response (EDR)	52%
Endpoint protection with both EDR and extensible provisioning protocol (EPP) in one package	31%
External threat intelligence platform (not just a data feed)	36%
Messaging security gateway/spam/phishing detection	34%
Network admission control	35%
Next-generation firewall	47%
Security automation and orchestration	40%
Security policy orchestration and automation	38%
SIEM	45%
Threat intelligence platform	36%
User awareness training such as anti-phishing and cybersecurity awareness	47%
VPN appliances	39%
Vulnerability management	38%
WAF	49%
Web security gateway	37%
Other (please specify)	2%
Total	886%

Q23. Which of the following governance practices does your organization implement? Please select all that apply.	Total
Engagement of managed security service provider	50%
Information/digital rights management and collaboration	50%
Risk management (internal)	55%
Third-party risk management	55%
Other (Please specify)	3%
Total	212%

Part 5. Your role and organization

D1. Experience	Total
Total years of relevant experience	9.26
Total years in current position	6.06

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	Total
CEO/executive committee	3%
Chief operating officer	1%
Chief information officer	44%
Chief technology officer	9%
Chief financial officer	0%
Leader, human resources	1%
Leader, business unit or LOB	9%
Leader, corporate compliance	3%
Leader, risk management	7%
Leader, IT administration	1%
Data center management	2%
Chief information security officer	18%
Chief security officer	2%
Total	100%

D3. What industry best describes your organization's primary sector?	Total
Agriculture & food services	0%
Communications	3%
Consumer products	5%
Defense & aerospace	0%
Education & research	1%
Energy & utilities	6%
Financial services	17%
Health & pharmaceutical	10%
Hospitality & leisure	1%
Industrial & manufacturing	11%
Public sector	10%
Retail	9%
Services	11%
Technology & software	9%
Transportation	4%
Other	1%
Total	100%

D4. What best describes your organization's geographic footprint?	Total
Domestic	15%
Primarily one global region	23%
Primarily two or more global regions	34%
All global regions (multinational)	28%
Total	100%

D5. What is the worldwide headcount of your organization?	Total
Less than 1,000	15%
1,000 to 5,000	25%
5,001 to 10,000	28%
10,001 to 25,000	18%
25,001 to 75,000	10%
More than 75,00	5%
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.