Ponemon INSTITUTE

The 2020 Study on Staffing the IT Security Function in the Age of Automation: United States and United Kingdom

Sponsored by DomainTools

Independently conducted by Ponemon Institute LLC

Publication Date: February 2020

The 2020 Study on Staffing the IT Security Function in the Age of Automation: United States and United Kingdom

Prepared by Ponemon Institute, February 2020

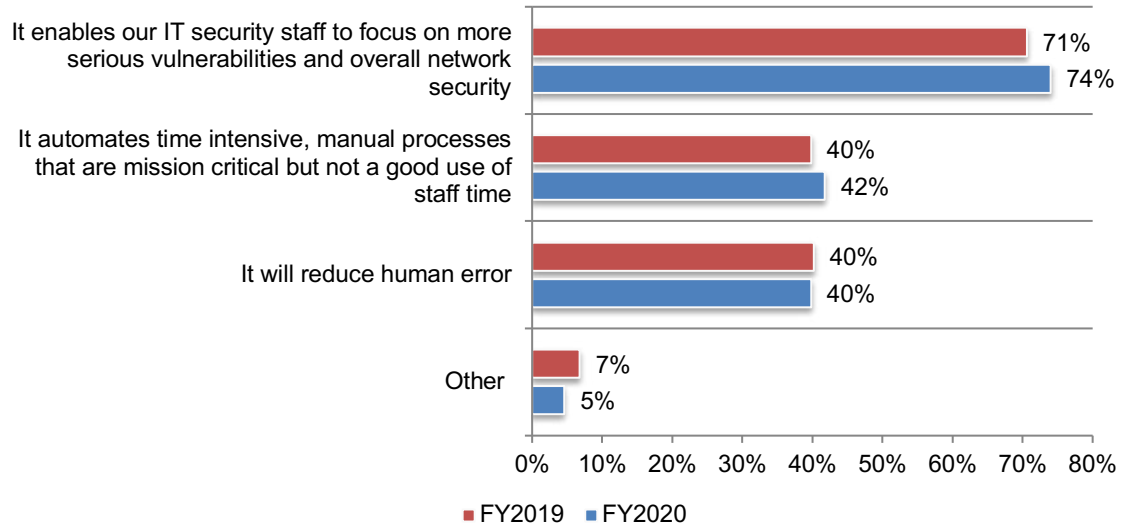
Part 1. Introduction

Ponemon Institute, with sponsorship from DomainTools, conducted *The 2020 Study on Staffing the IT Security Function in the Age of Automation*[1] to identify the challenges to having the necessary in-house expertise to achieve a strong cybersecurity posture. Ponemon surveyed 1,027 IT and IT security practitioners in the United States (617) and the United Kingdom (410) 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. This report presents the 2019 and 2020 consolidated findings for the US and UK.

While the lack of in-house IT security expertise continues to be a problem, the key takeaway in this year's study is that the majority of respondents (51 percent) now believe that automation will decrease headcount in the IT security function, an increase from 30 percent in last year's study. Further, more respondents believe they will lose their jobs in an average of four years, an increase from 28 percent of respondents to 37 percent of respondents since last year. Possible reasons for these perceptions are that automation, according to the findings, can improve the effectiveness and efficiency of the IT security staff so in the future fewer will need to be hired.

With automation, the IT security staff is able to focus on more serious vulnerabilities. Seventy-six percent of respondents say their organizations currently use or plan to use automation. According to these respondents, the most valuable feature is the ability to have the IT security staff focus on the more serious vulnerabilities and overall network security, (74 percent of respondents). Because of staffing shortages, 42 percent of respondents say it is a benefit to have time intensive and manual processes automated that are mission critical but not a good use of their staff's time.

Figure 1. How will automation improve the ability of their IT security staff to do their jobs?
More than one response permitted



[1] Automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence (AI), machine learning and orchestration. Artificial intelligence refers to the development of computer systems that are able to perform tasks normally requiring human intelligence.

Following are other key takeaways from the research

- Barriers to investing in automation continue to be the lack of in-house expertise (53 percent of respondents) and a heavy reliance on legacy IT environments.

- Automation increases the productivity of current security personnel (43 percent of respondents) and reduces the false positive and/or false negative rates (43 percent of respondents). Sixty percent of respondents say automation is helping to reduce the stress of their organization's IT security personnel.

- Automation will improve productivity but the human factor is still important. Seventy-four percent of respondents say automation is not capable of performing certain tasks that the IT security staff can do and 54 percent of respondents say automation will never replace human intuition and hands-on experience.

- Seventy-two percent of respondents say their organizations have resources that focus on threat detection. The threat intelligence typically consumed are network traffic, firewall/IPS traffic and threat intelligence sources.

- GDPR, China Internet Security Law, APEC Privacy Framework and other regulations are influencing the adoption of automation, according to 72 percent of respondents, an increase from 66 percent of respondents in last year's study. Similarly, among the knowledge required of highly experienced job candidates is familiarity with security regulations and standards (81 percent of respondents).

- Attackers are increasing their use of automation. Fifty-three percent of respondents say they are seeing a growth in attackers' use of automation, an increase from 47 percent of respondents in last year's research.

Part 2. Key findings

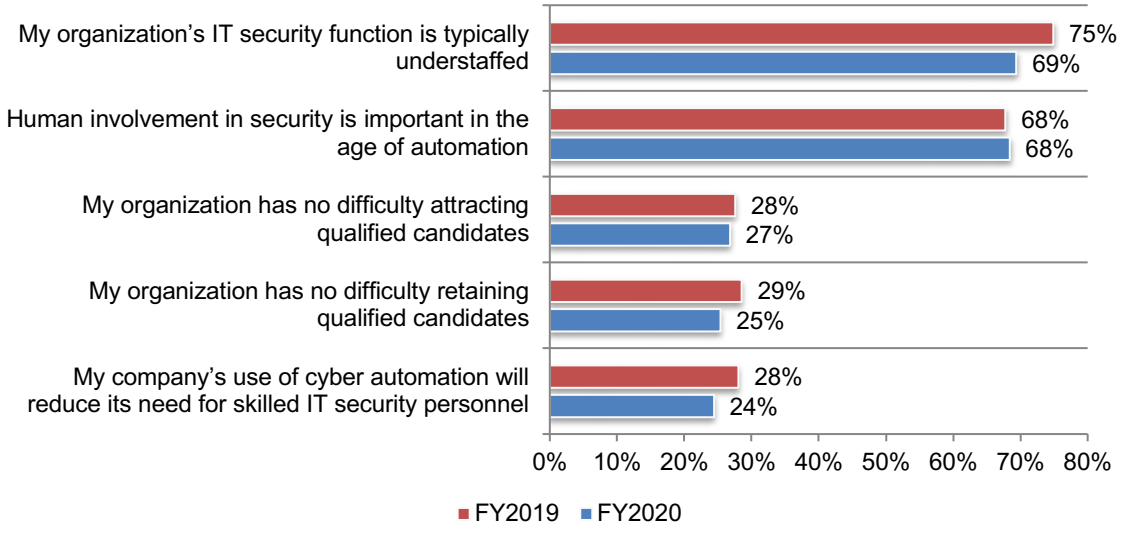
This section presents a detailed analysis of the research. The complete audited findings are presented in the Appendix of this report, which is organized according to the following topics:

- Automation and the future of IT security staffing
- The IT security team's use of threat intelligence and other technologies
- What entry-level and senior IT security practitioners need to know
- Differences by industry and organizational size
- Differences between the US and UK

How automation influences the staffing of the IT security function

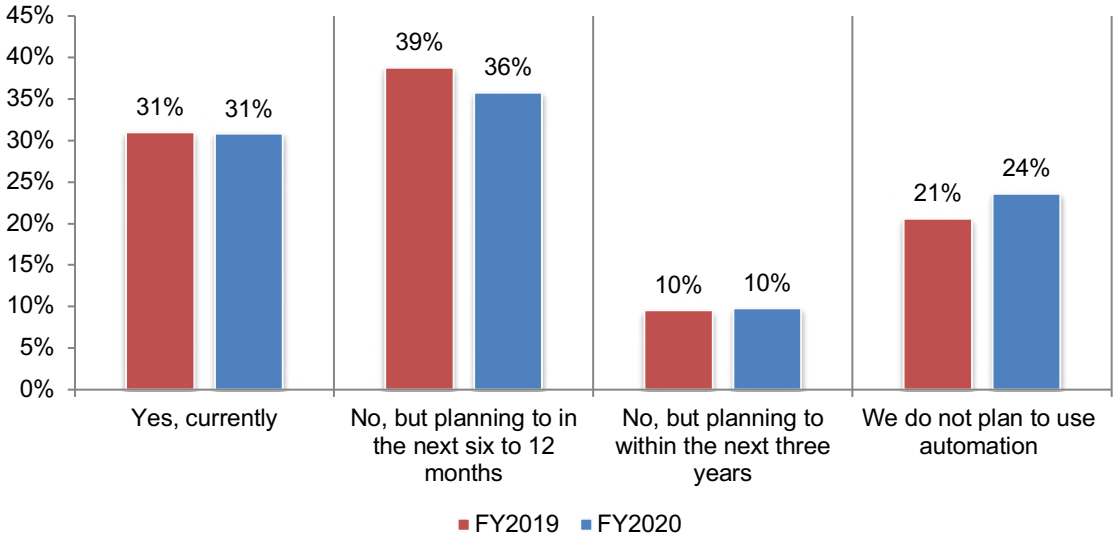
Staffing the IT security function improves slightly. According to Figure 2, 69 percent of respondents say their organizations' IT security function is typically understaffed, a decrease from 75 percent in last year's study. Most respondents still believe that human involvement in security is important in the age of automation (68 percent of respondents) and it will not reduce the need for skilled IT security personnel.

Figure 2. Perceptions about the hiring and retention of IT security
Strongly agree and Agree responses combined



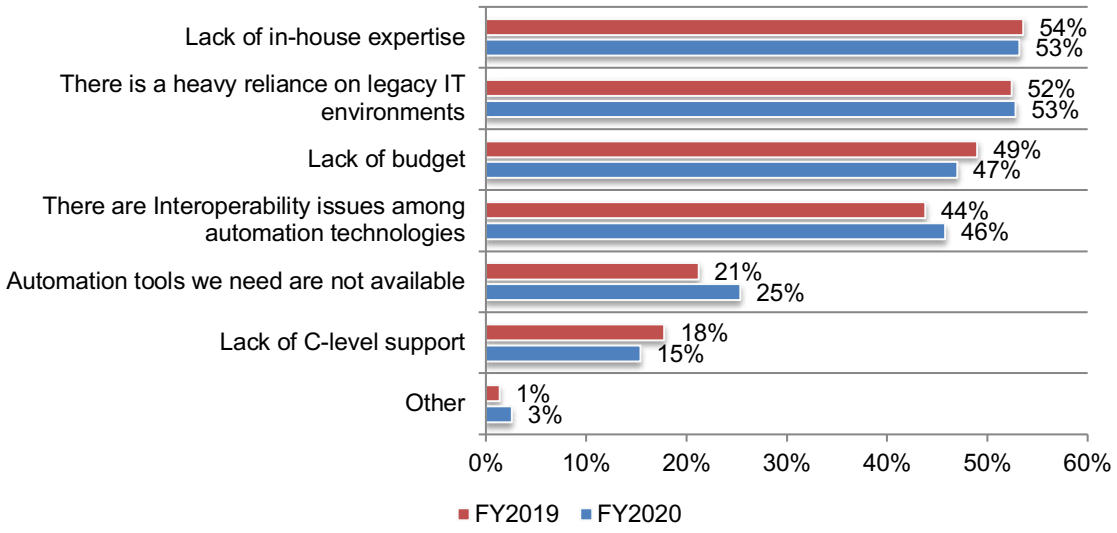
The benefits of automation drive investment in these technologies. As shown in Figure 3, 77 respondents either use automation currently or plan to in the future. A very slight decrease from 80 percent of respondents in last year's research. As discussed above, these investments will make better use of the IT security staff's time by enabling them to focus on the most serious security threats.

Figure 3. Does your organization use automation?



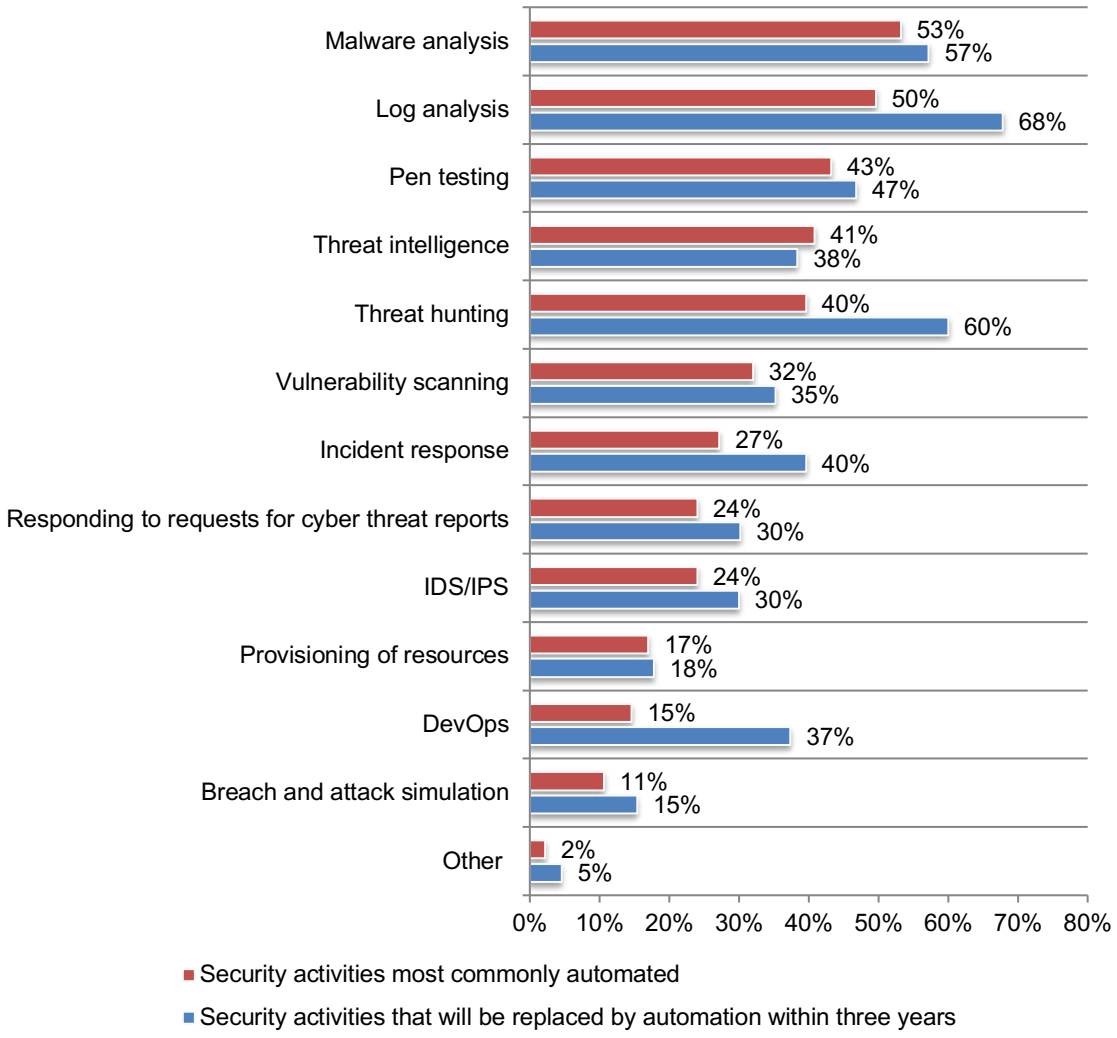
The lack of in-house expertise and legacy IT environments affects the adoption of automation. As Figure 4 shows, of the 24 percent of respondents who have no plan to adopt automation in their organizations, 53 percent say their choice is due to not having the necessary skilled IT security practitioners to manage these solutions. A further 53 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



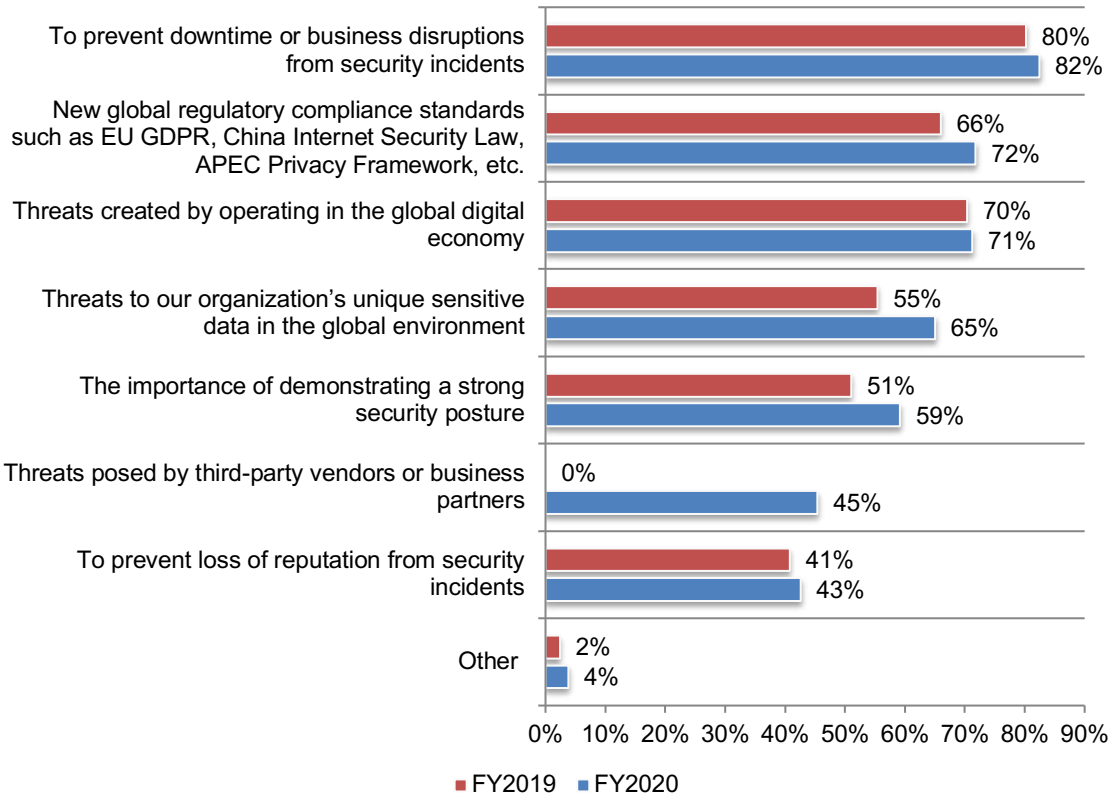
Log analysis and threat hunting are the most common security activities automated. As reported previously, 77 percent of respondents say their organizations currently use or plan to use automation within the next three years. Since last year's study, there have been significant increases in the likelihood of automating log analysis, threat hunting, incident response and DevOps, 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



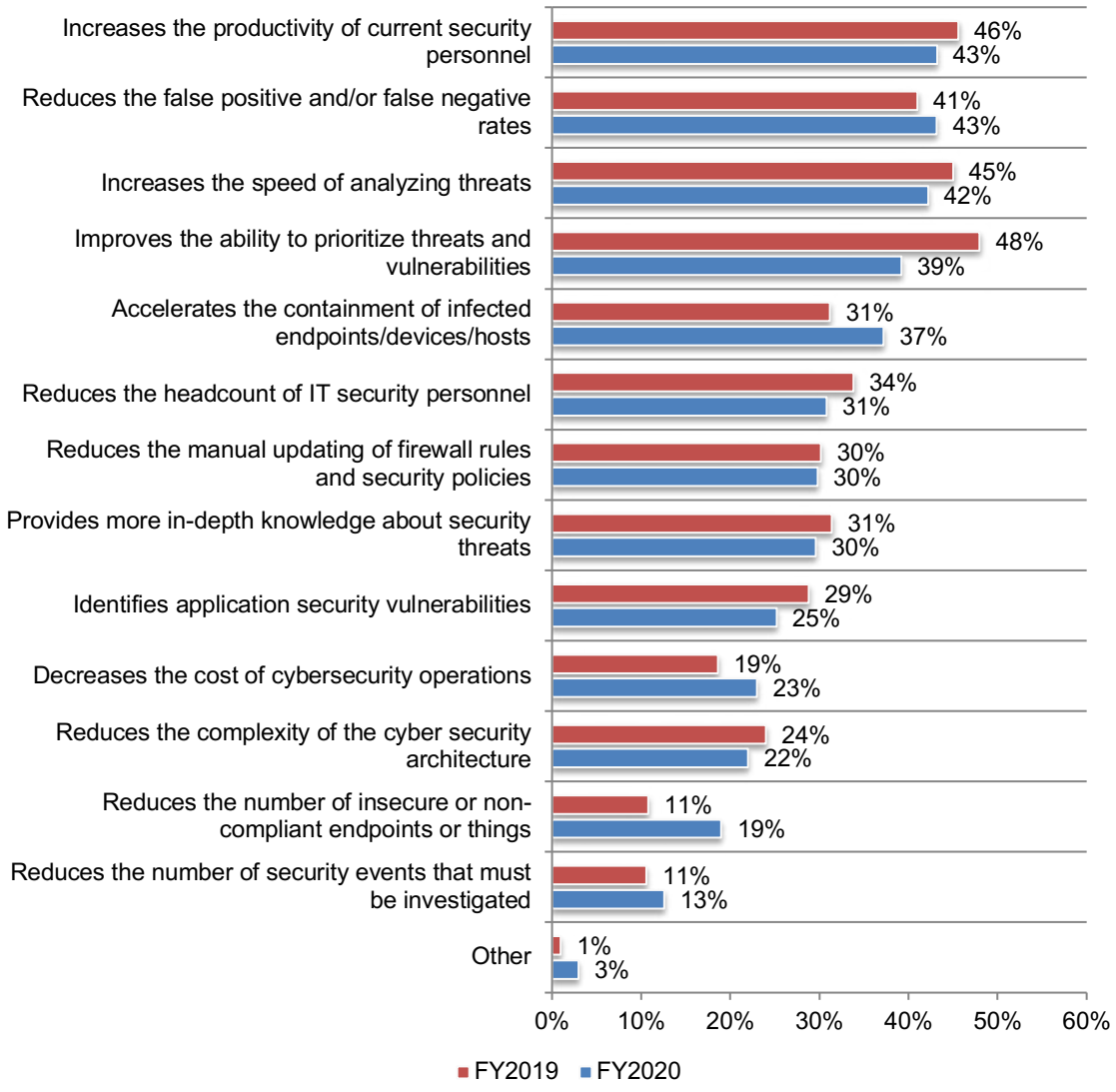
Preventing downtime and complying with global regulatory compliance standards are incentives to automate. Similar to last year's study, prevention of downtime caused by business disruptions from security incidents (82 percent of respondents) are reasons to automate. This year, the ability to comply with global regulatory compliance standards, threats to sensitive data in the global environment and the importance of demonstrating a strong security posture have increased significantly.

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



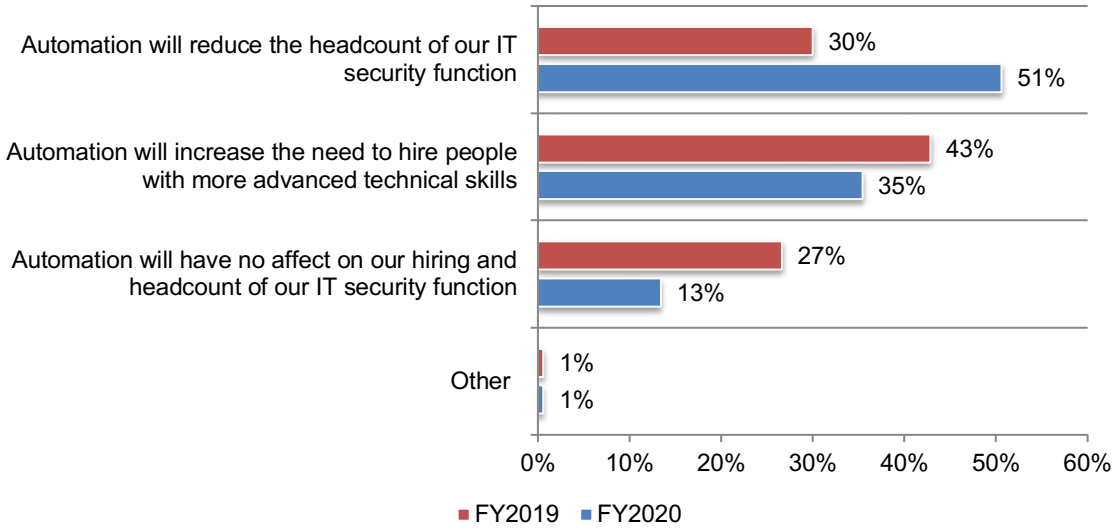
Automation makes the IT security function more efficient. Productivity is critical to overcoming the disadvantage of not having sufficient in-house expertise. As shown in Figure 7, the reduction of false positives and/or false negative rates and the speed of analyzing threats contributes to improvements in productivity. However, few respondents say it reduces the complexity of the cybersecurity architecture, the number of insecure or non-compliant endpoints or IoT and the number of security events that must be investigated.

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



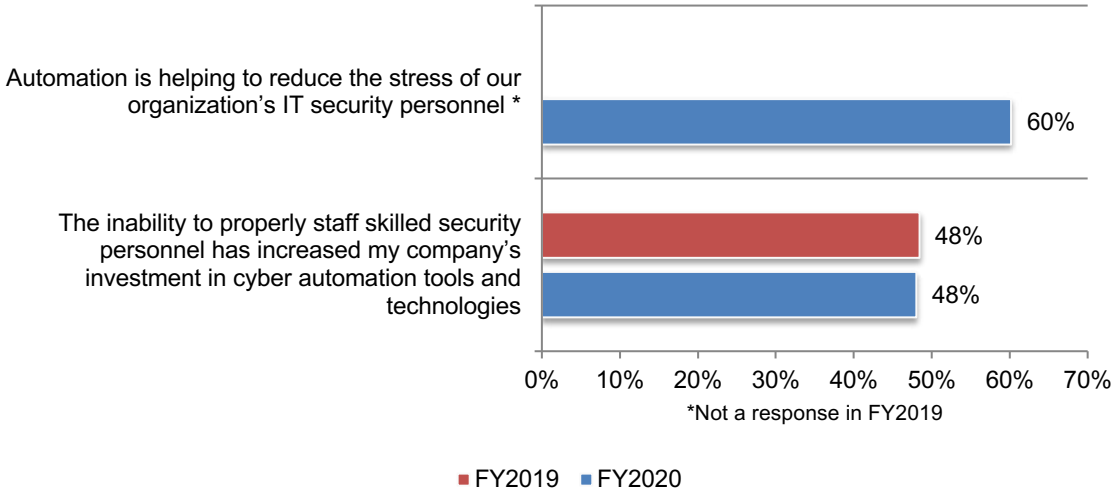
Automation will affect the hiring of IT security professionals. Since last year's study, there has been a significant shift in perceptions about how automation will affect the hiring of IT security personnel. In contrast to last year, more than half of respondents (51 percent) predict automation will reduce the headcount and the need to hire people with more advanced technical skills has decreased from 43 percent of respondents to 35 percent, as shown in Figure 8.

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



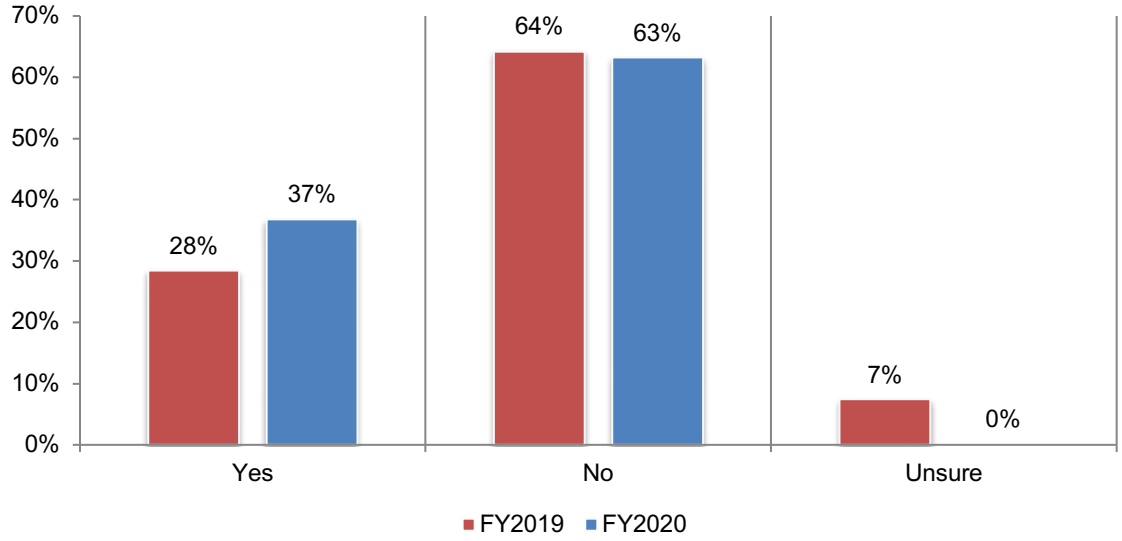
In addition to making the IT security staff more efficient, automation also reduces the stress of IT security personnel, as shown in Figure 9. Almost half (48 percent of respondents) say the shortage of in-house expertise has increased their companies' investment in cyber automation tools and technologies.

Figure 9. Automation and staffing
Strongly agree and Agree responses combined



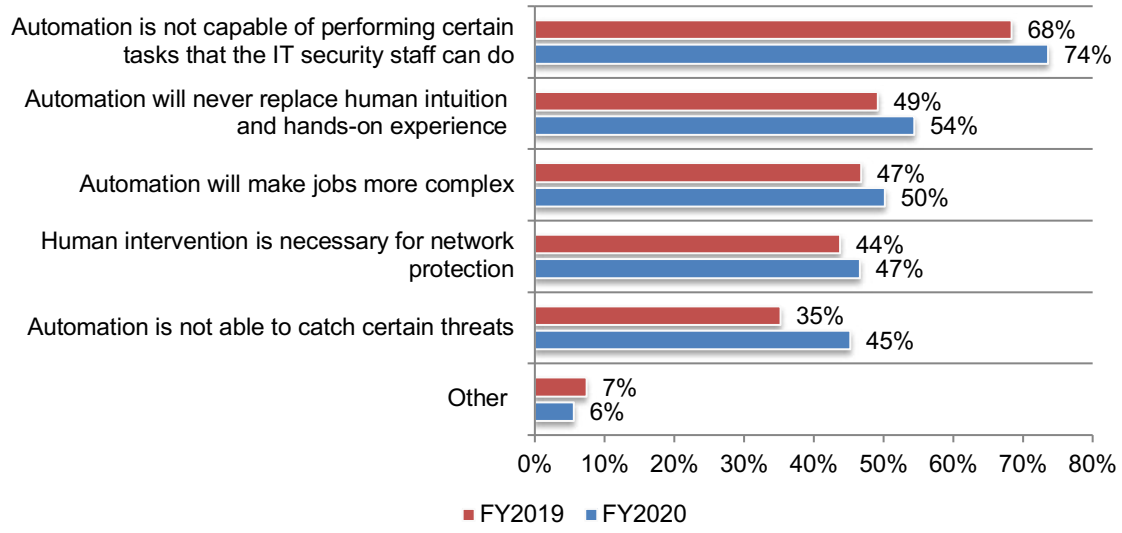
Concerns about losing their jobs because of automation has increased. As discussed above, the majority of respondents believe headcount will be affected by automation. As shown in Figure 10, 37 percent of respondents believe they will lose their jobs as a result of automation, an increase from 28 percent of respondents in 2019. Of the 37 percent who say they are concerned about keeping their job, the majority believe this will happen in an average of 4 years.

Figure 10. Do you personally think you will lose your job because of automation?



Automation is expected to improve productivity but will not replace the human factor. As shown in Figure 11, 74 percent of respondents say automation is not capable of performing certain tasks that IT security staff can do, while 54 percent of respondents maintain that it will never replace human intuition and hands-on experience.

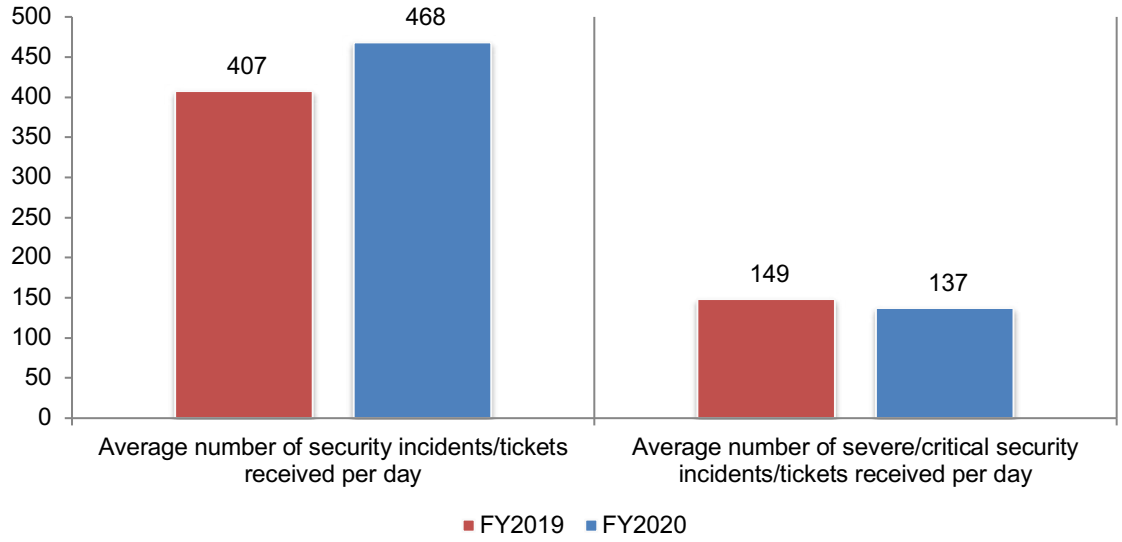
Figure 11. How will automation *not* improve your IT security staff's ability to do their job?
More than one response permitted



The IT security team's use of threat intelligence and other technologies

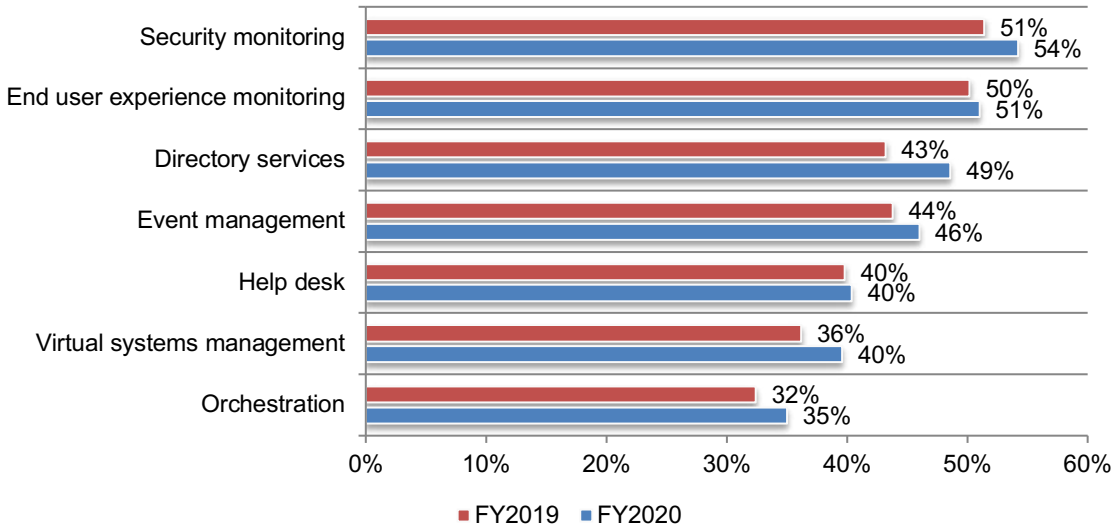
Security incidents/tickets increase significantly, putting stress on the IT security staff. According to Figure 12, since last year the average number of security incidents/tickets has increased from 407 to 468. The average number of severe/critical security incidents/tickets received per day has decreased.

Figure 12. The average number of security and severe security incident/tickets the security team receives each day
Extrapolated values presented



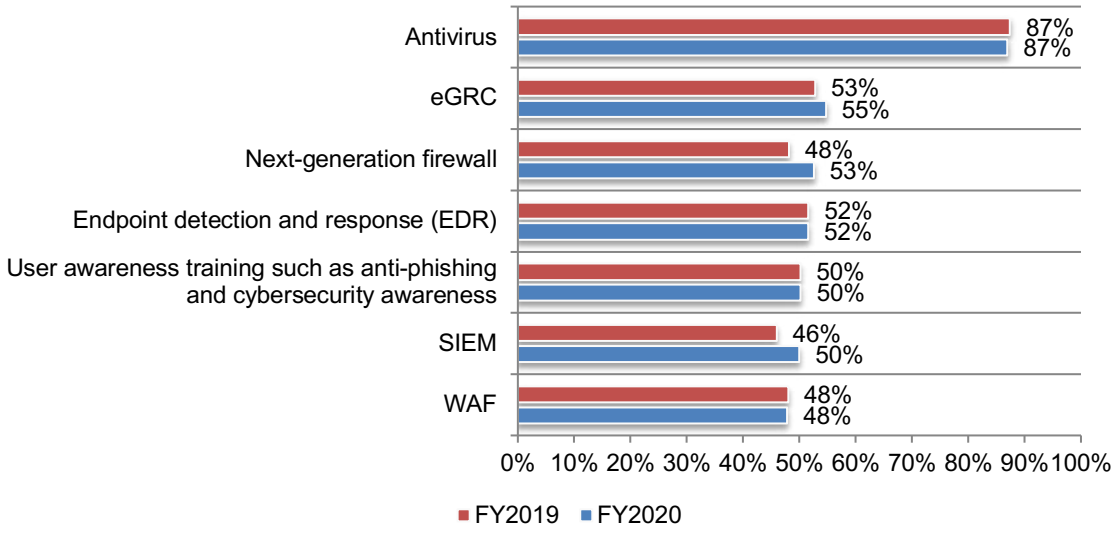
Monitoring technologies are the solutions most often integrated with organizations' security management tools. According to Figure 13, security monitoring and end-user experience monitoring are in the top 7 of solutions integrated in security management tools. This year, directory services has increased from 43 percent of respondents to 49 percent of respondents.

Figure 13. The top 7 solutions integrated with organizations' security management tools
More than one response permitted



Antivirus continues to be the number one technology solution used today. As shown in Figure 14, more organizations are using eGRC.

Figure 14. The top 7 security technology solutions deployed today
More than one response permitted



Seventy-two percent of respondents say their organizations have resources that focus on threat detection. As shown in Figure 15, 37 percent of respondents say their organizations either have a single dedicated person (18 percent) or a formal dedicated team (19 percent).

Figure 15. Does your organization have resources that focus on threat detection?

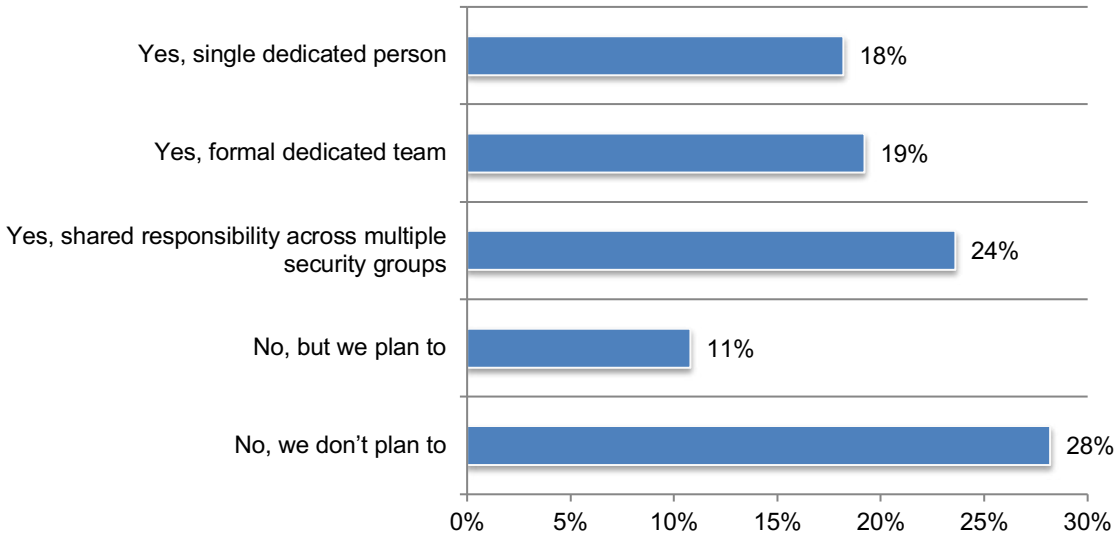
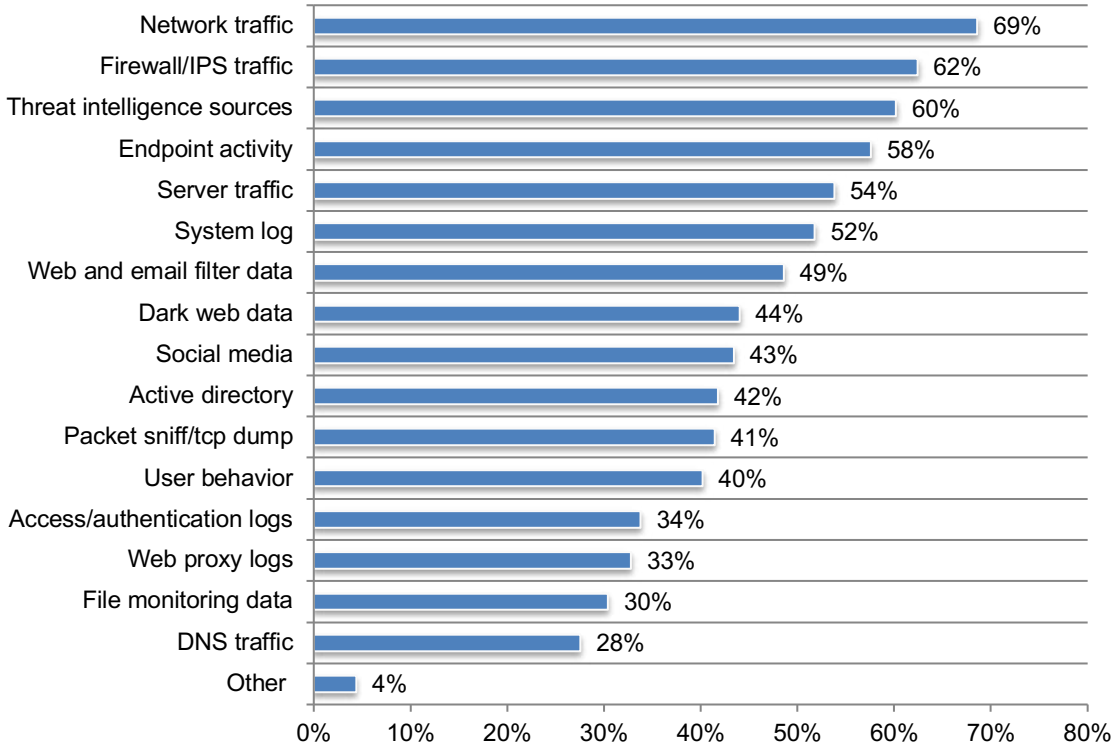


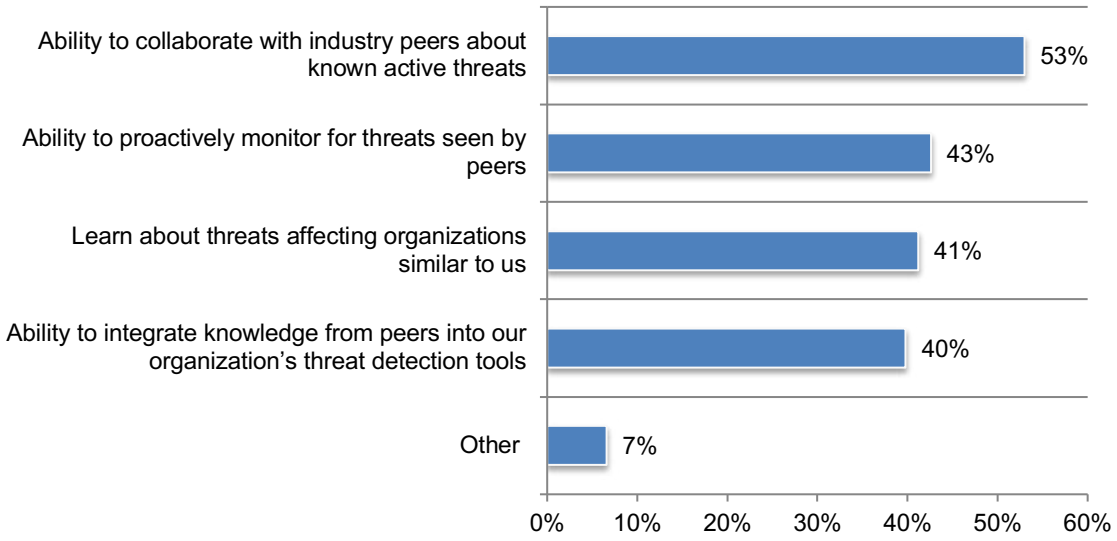
Figure 16 presents the threat intelligence typically consumed by organizations. The top three types of threat intelligence of value to organizations are network traffic, firewall/IPS traffic and threat intelligence sources.

Figure 16. If yes, what threat intelligence does your organization consume?
More than one response permitted



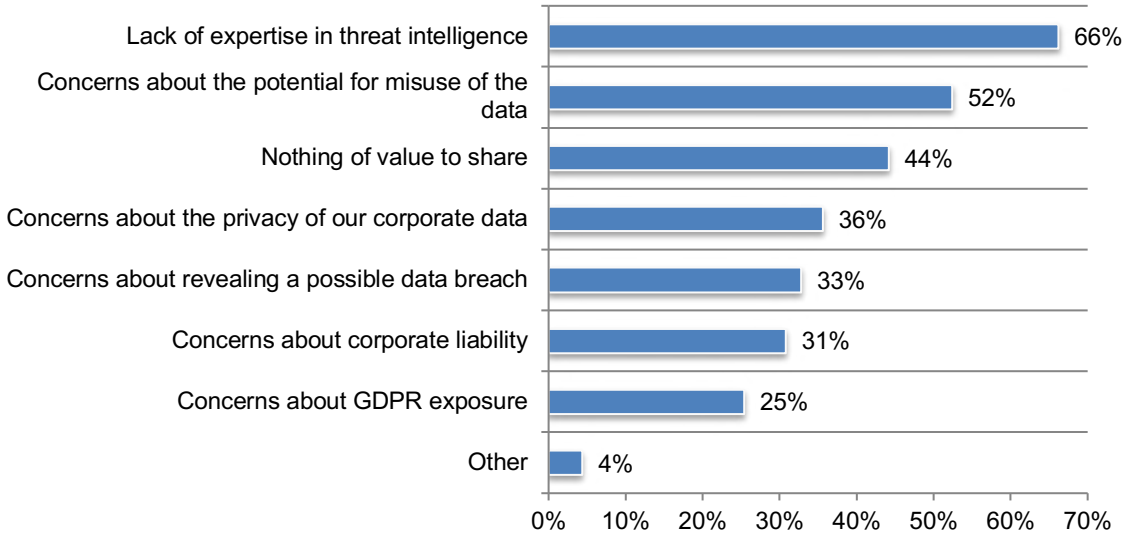
Organizations are sharing threat intelligence to collaborate with industry peers. Almost half of respondents (48 percent) are engaging in threat sharing. According to Figure 17, 53 percent of respondents say the ability to collaborate with industry peers about known active threats is the benefit of sharing intelligence.

Figure 17. If yes, what are the benefits of sharing intelligence with other groups?
More than one response permitted



Of the 51 percent of respondents who do not share, the primary reason, according to Figure 18, is the lack of expertise followed by concerns about the potential misuse of the data.

Figure 18. If no, why doesn't your organization share threat intelligence with other organizations?
More than one response permitted



What entry-level and senior IT security practitioners need to know

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 far more knowledgeable about a wide range of governance and technology issues. These include experience with intrusion prevention and detection systems, familiarity with security regulations and standards and understanding information security frameworks.

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

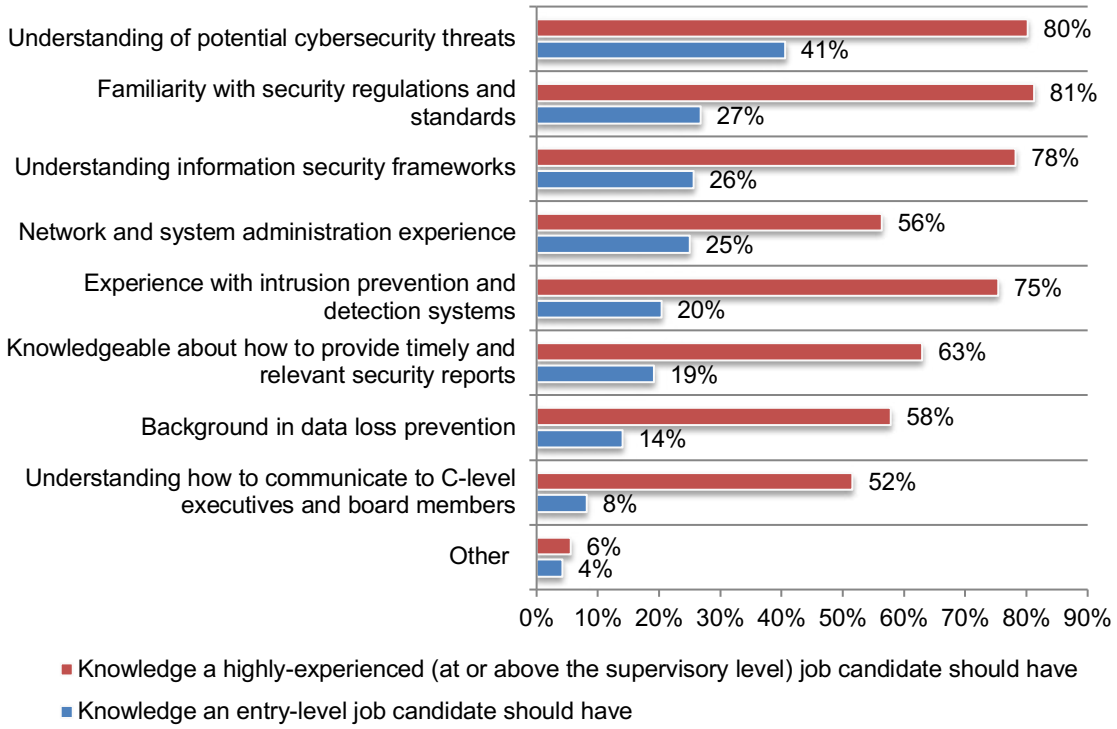
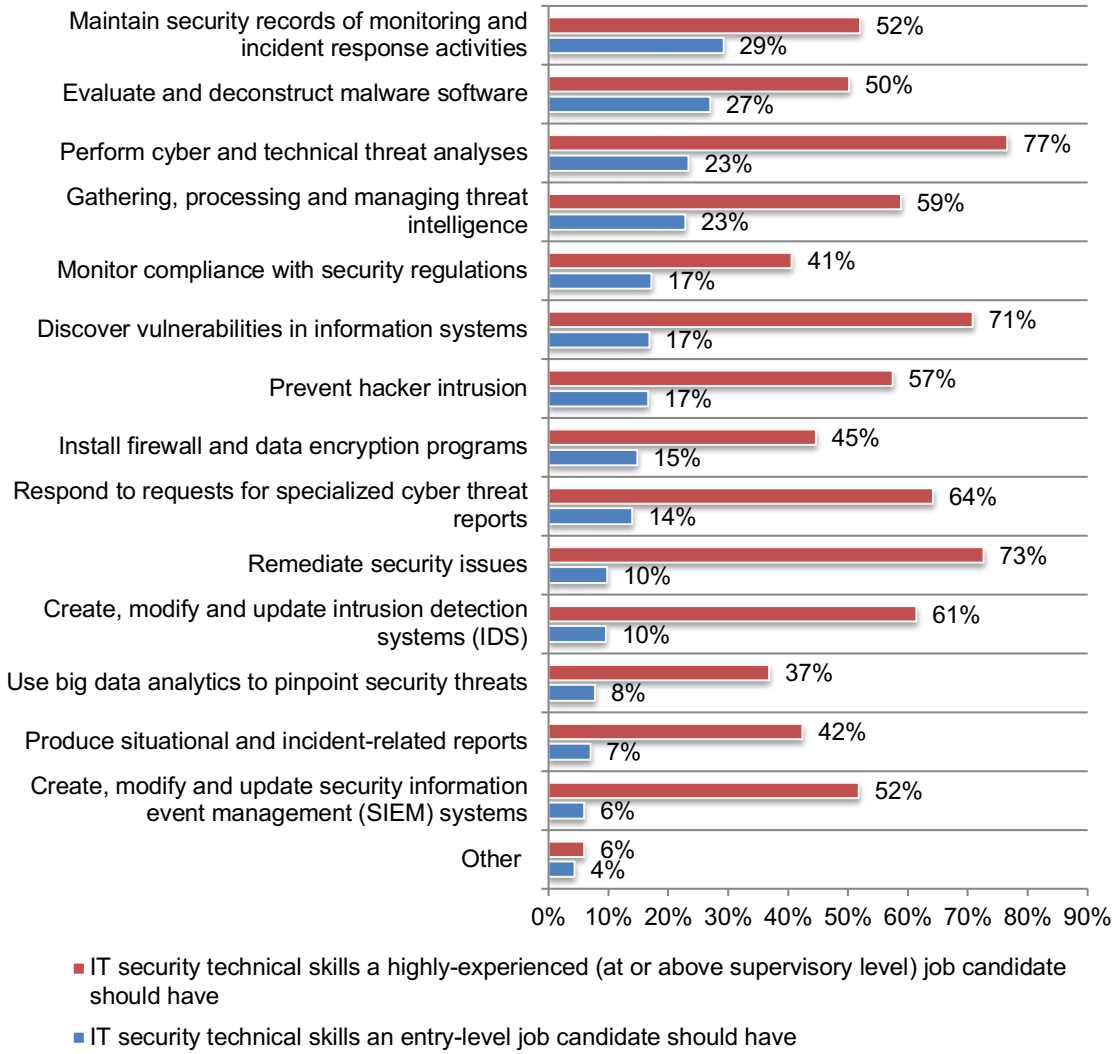


Figure 20 shows that entry-level job candidates are expected to have more tactical technical skills, such as maintaining security records of monitoring and incident response activities and evaluating and deconstructing malware software. Highly experienced job candidates, on the other hand, are mostly expected to be able to remediate security issues, perform cyber and technical threat analyses, discover vulnerabilities in information systems 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

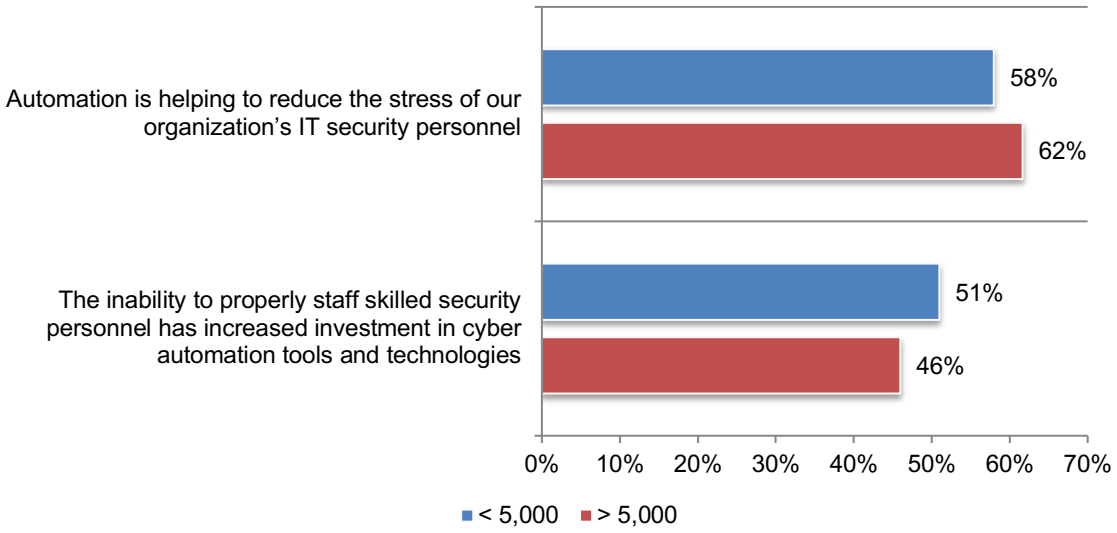


Organizational size and automation

To understand how organizational size affects the use of automation, we did a special analysis of respondents in a worldwide headcount of less than 5,000 (40 percent of respondents) and more than 5,000 (60 percent of respondents). Following are some of the most interesting differences.

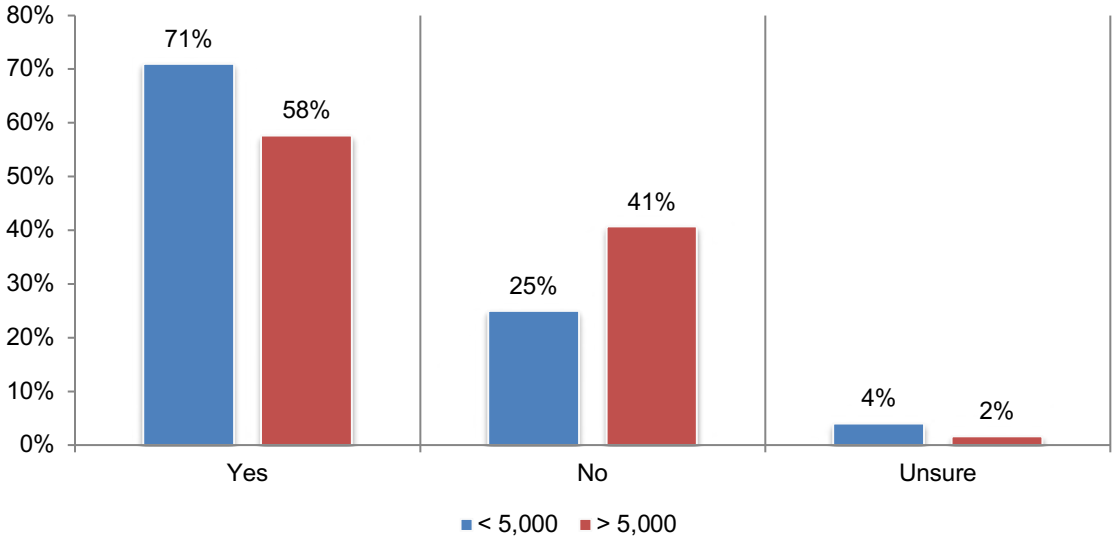
Automation is more likely to reduce the IT security staff's stress in large organizations (62 percent of respondents vs. 58 percent of respondents. Smaller organizations are more likely to increase investment in cyber automation tools and technologies to supplement their security staff (51 percent of respondents vs. 46 percent of respondents), as shown in Figure 21.

Figure 21. Perceptions about automation
Strongly agree and Agree responses combined



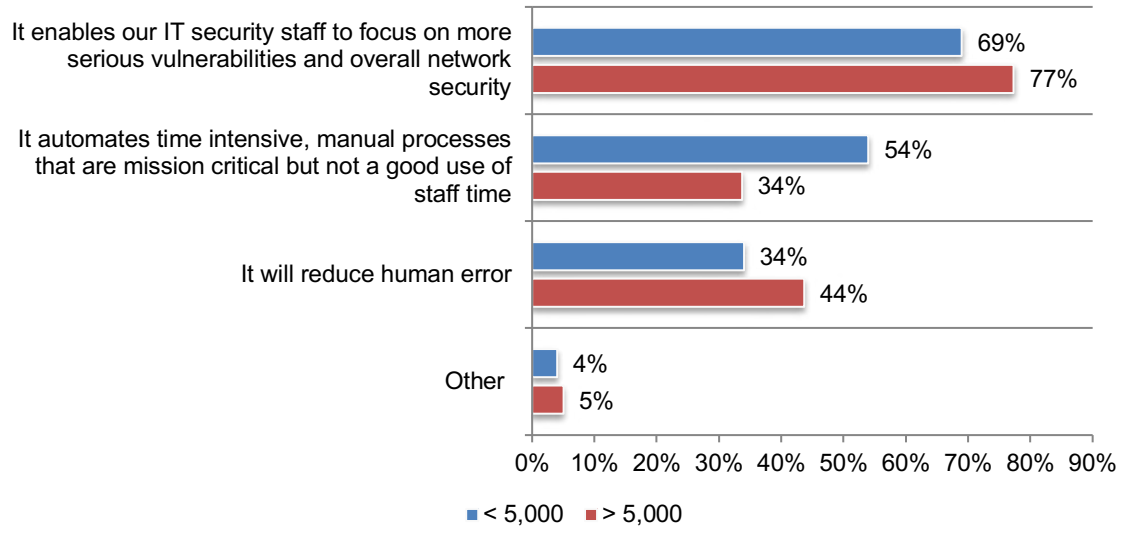
As shown in Figure 22, automation is considered more likely to improve the ability of the IT security staff to do their jobs in smaller organizations (71 percent vs. 58 percent of respondents).

Figure 22. Does automation improve your IT security staff's ability to do their jobs?



If automation is considered to improve the ability to do their jobs, the primary reason is that it enables the IT security staff to focus on more serious vulnerabilities and overall network security. Respondents in smaller organizations are more likely to see the benefit from automating time intensive, manual processes (54 percent vs. 34 percent of respondents), as shown in Figure 23.

Figure 23. Why does automation improve your IT security staff's ability to do their jobs?
More than one response permitted

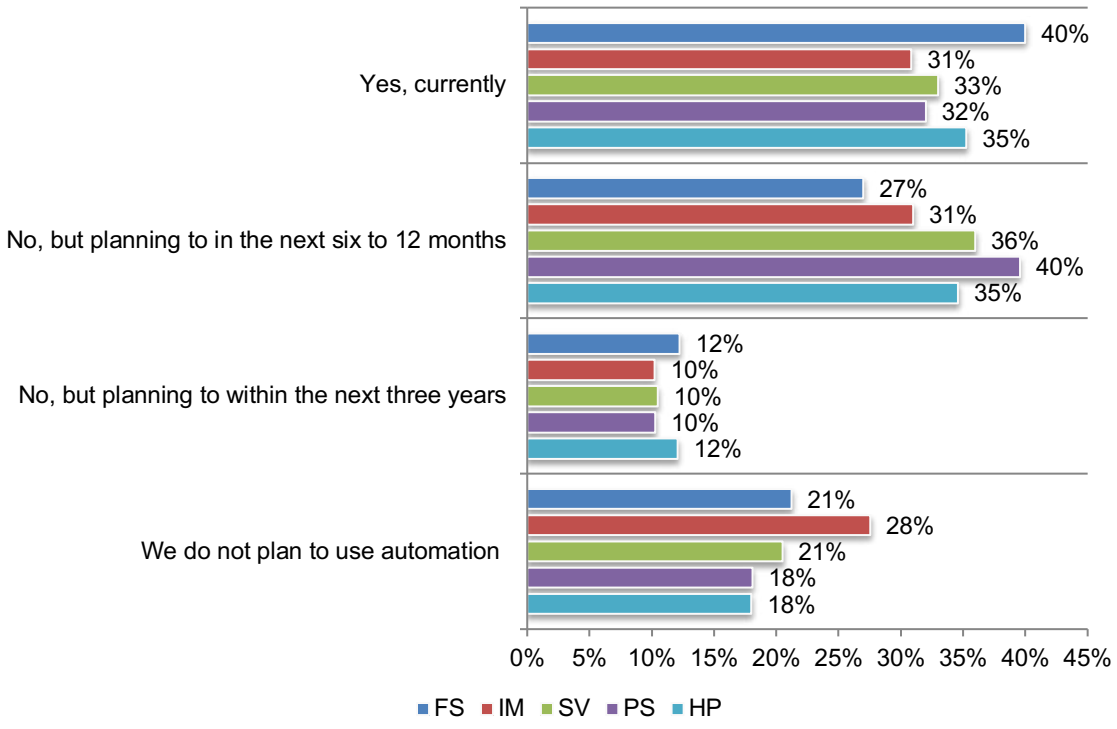


Industry differences in automation

We also analyzed the differences among the following industries represented in this research: financial services (FS), industrial/manufacturing (IM), services (SV), public sector (PS) and health and pharmaceutical (HP).

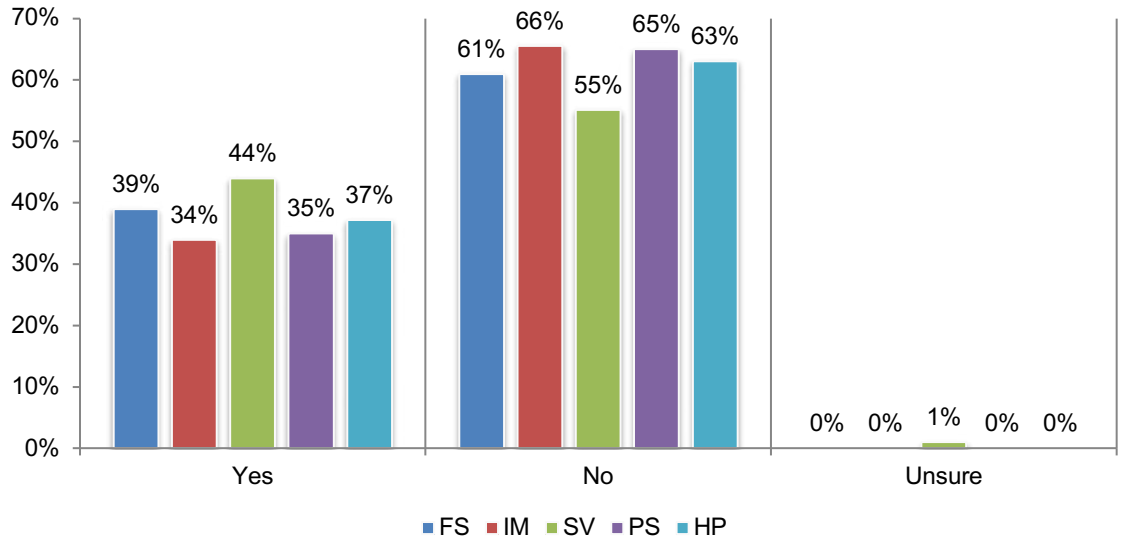
More respondents in financial services (40 percent) say their organizations are currently using automation, according to Figure 24. Industrial/Manufacturing respondents are more likely not to use automation.

Figure 24. Does your organization use automation?



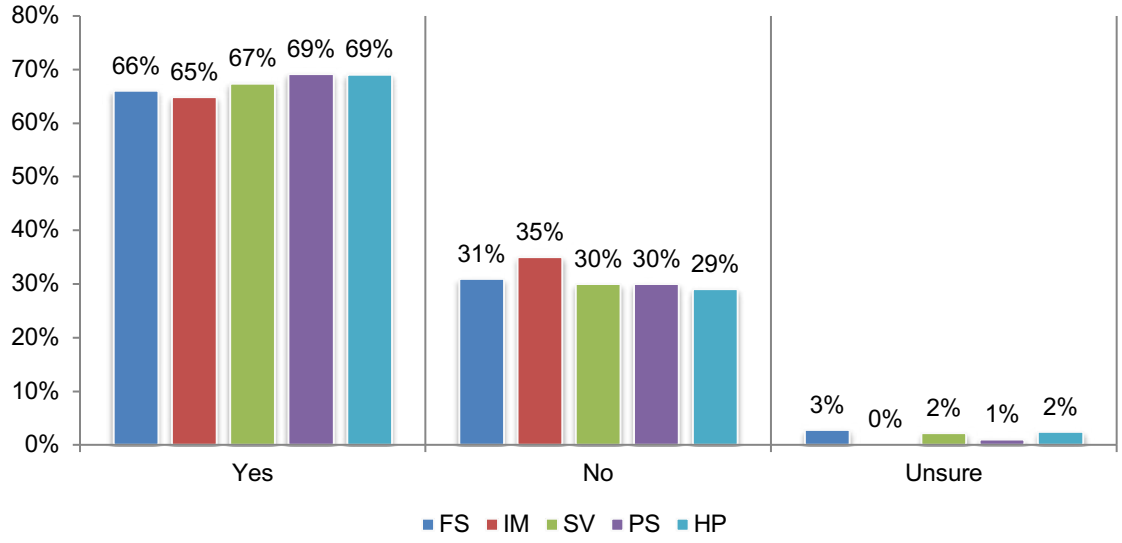
Respondents in the services industry are more likely to think they will lose their job because of automation, as shown in Figure 25. The most optimistic they will not lose their jobs are respondents in industrial/manufacturing and the public sector.

Figure 25. Do you personally think you will lose your job because of automation?



According to Figure 26, almost all respondents in every industry believe automation improves their IT security staff's ability to do their jobs.

Figure 26. Does automation improve your IT security staff's ability to do their jobs?

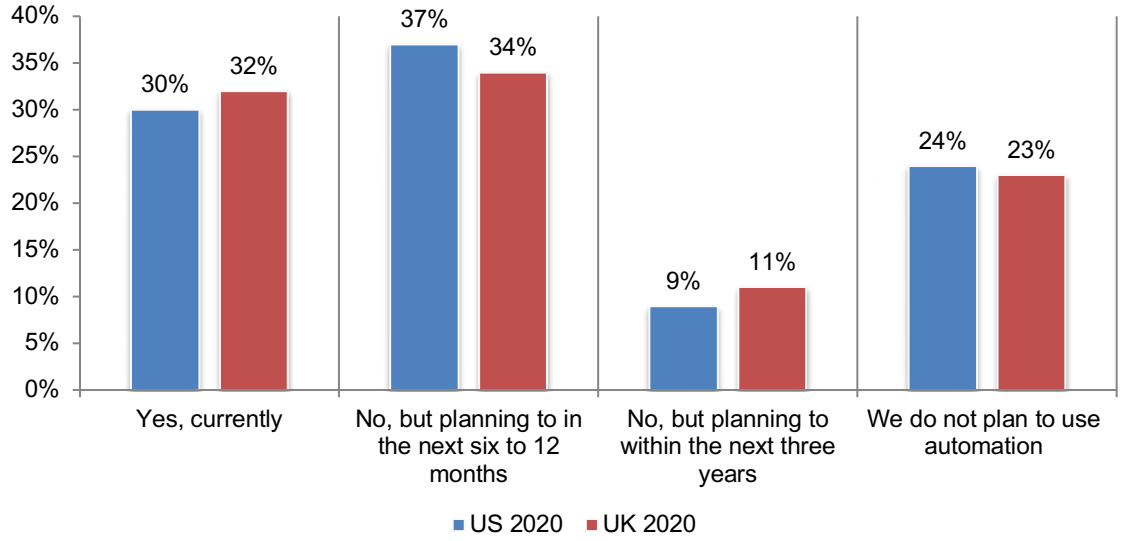


Differences between US and UK findings

In this section we present differences between the US (617 respondents) and UK findings (410 respondents).

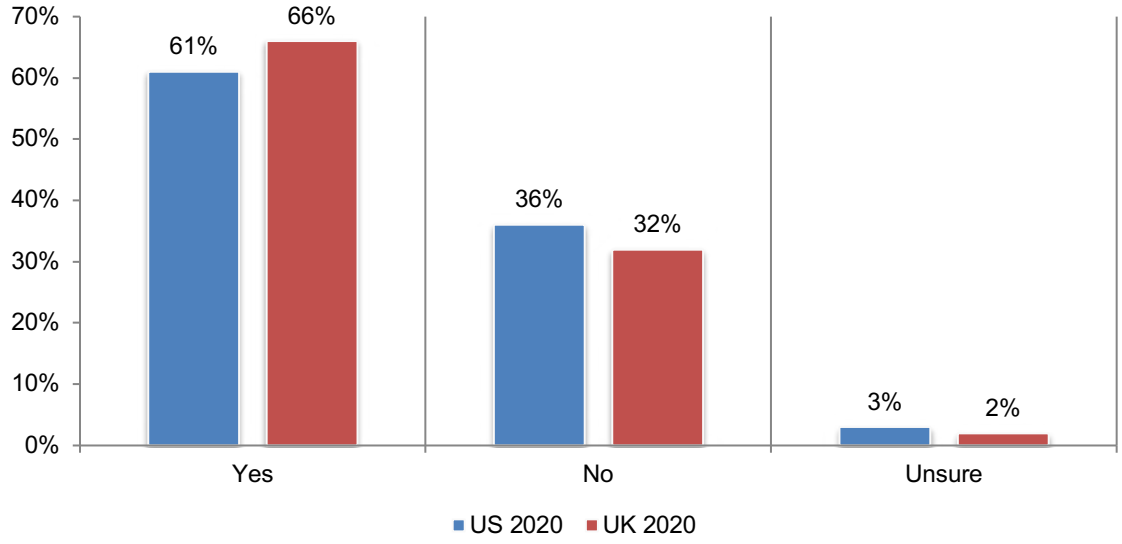
Most US (76 percent of respondents) and UK organizations (77 percent of respondents) currently or plan to adopt automation, as shown in Figure 27.

Q27. Does your organization use automation?



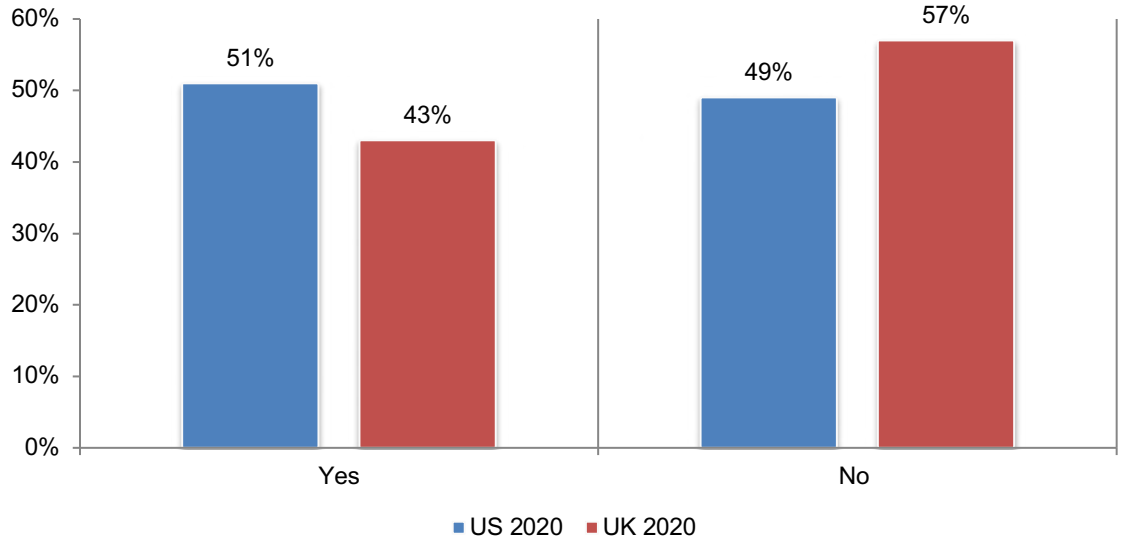
UK organizations are more likely to believe automation improves their IT security staff's ability to do their jobs (66 percent vs. 61 percent of respondents), according to Figure 28.

Q28. Does automation improve your IT security staff's ability to do their jobs?



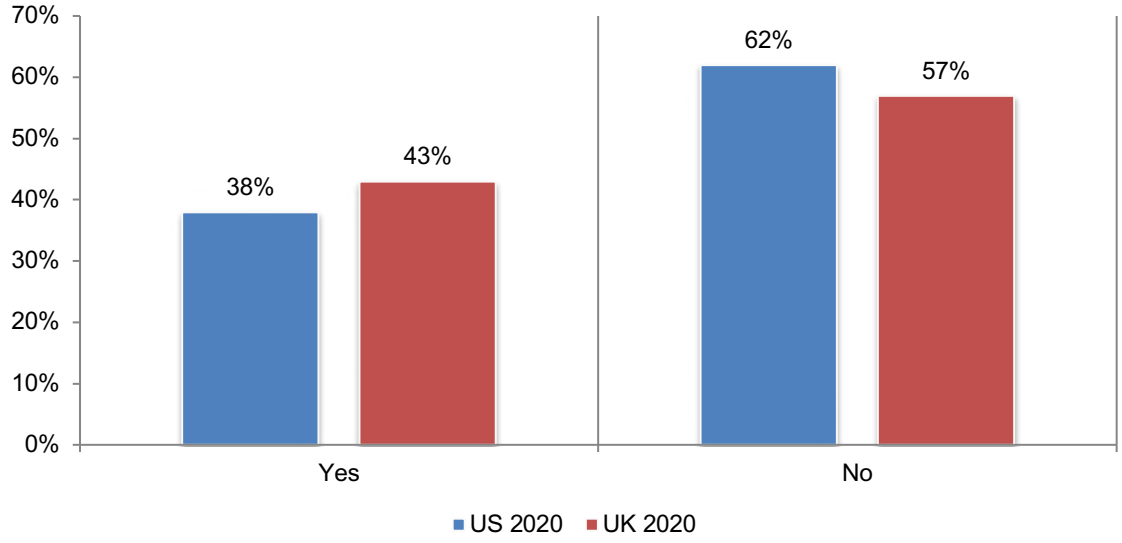
According to Figure 29, US organizations are more likely to use threat intelligence in its cybersecurity program (51 percent vs. 43 percent of respondents).

Q29. Does your organization use threat intelligence in its cybersecurity program?



UK organizations are more likely to brief the CEO and board of directors on its use of automation, according to Figure 30.

Figure 30. Are your organization's CEO and/or board of directors briefed on its use of automation?



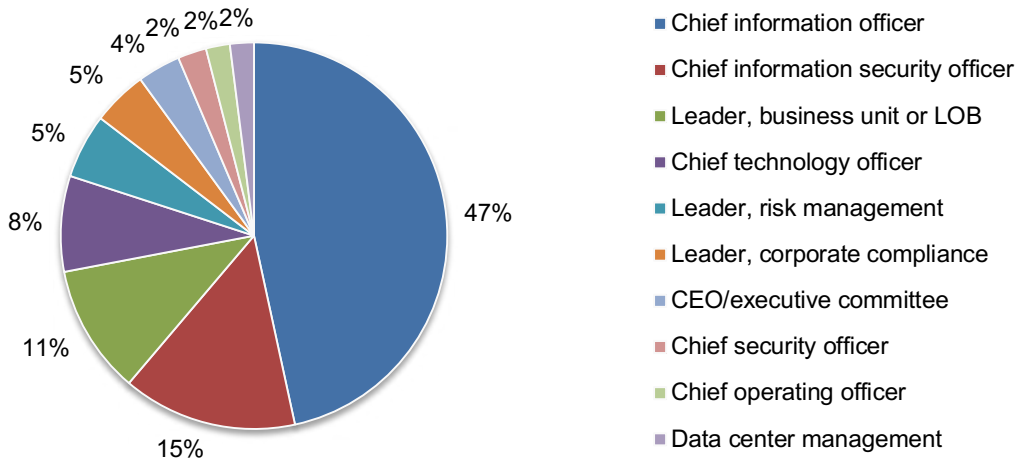
Part 3. Methods

A sampling frame of 26,443 IT and IT security practitioners located in the US, and the UK, 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 1,145 total returns. Screening and reliability checks required the removal of 118 surveys. Our final sample consisted of 1,027 surveys, or a 3.9 percent response rate. Respondents have been at their current position for an average of 6.5 years and have an average of 9.3 years of relevant experience.

Table 1. Sample response	FY2020	FY2019
Sampling frame	26,443	27,441
Total returns	1,145	1,143
Rejected or screened surveys	118	108
Final sample	1,027	1,035
Response rate	3.9%	3.8%

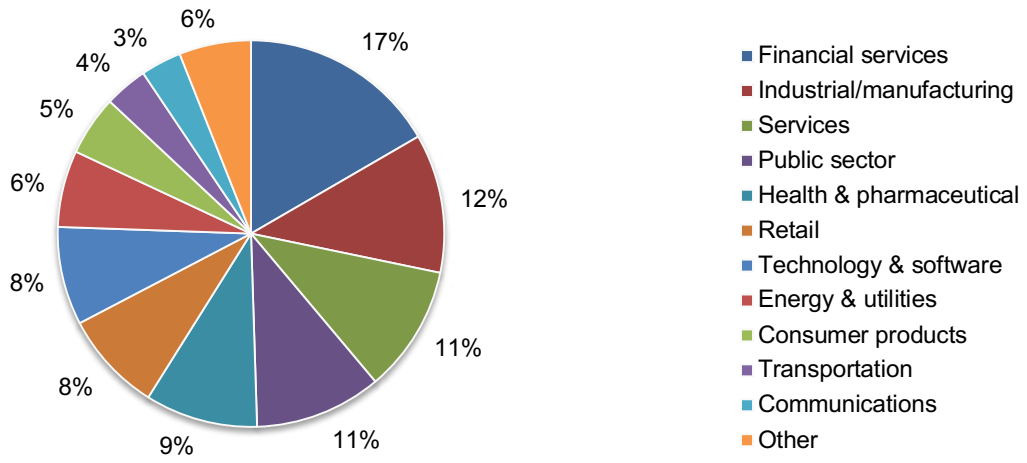
As shown in Pie Chart 1, 47 percent of respondents report to the chief information officer, 15 percent of respondents report to the chief information security officer, 11 percent of respondents report to the business unit leader and 8 percent of respondents indicated they report to the chief technology officer.

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



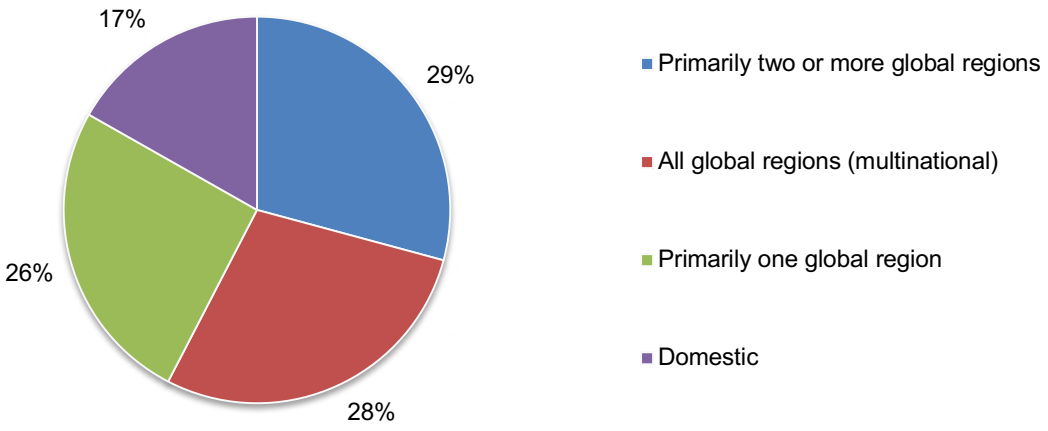
Pie Chart 2 reports the industry segments of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial and manufacturing (12 percent of respondents), services sector (11 percent of respondents), public sector (11 percent of respondents) and health and pharmaceuticals (9 percent of respondents).

Pie Chart 2. Industry distribution of respondents' organizations



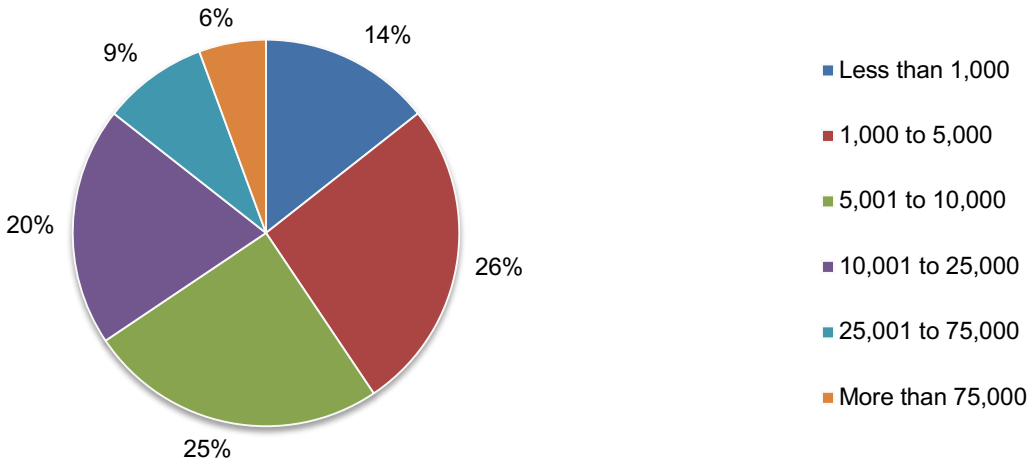
Pie Chart 3 reports the geographic footprint of the respondents' organizations. Twenty-nine percent of respondents are from organizations with a geographic footprint of primarily two or more global regions, 28 percent of respondents are from multinational organizations, 26 percent are from organizations with primarily one global region and 17 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 (60 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 between November 25 and December 12, 2019.

Survey response	FY2020	FY2019
Total sampling frame	26,443	27,441
Total returns	1,145	1,143
Rejected surveys	118	108
Final sample	1,027	1,035
Response rate	3.9%	3.8%
Sample weight	1.0	1.0

Part 1. Screening Questions

S1. What best describes your role/title in the organization? Please select only **one** choice.	FY2020	FY2019
Chief information officer (CIO)	9%	6%
Chief information security officer (CISO)	8%	7%
Chief risk officer (CRO)	3%	3%
Chief security officer (CSO)	3%	2%
Chief technology officer (CTO)	3%	2%
Infrastructure engineer (security/systems)	2%	1%
IT administrator	1%	1%
IT architect	1%	2%
IT business analyst	2%	1%
IT consultant/Integrator	3%	3%
IT director	13%	12%
IT manager	9%	10%
IT project/program manager	4%	4%
IT security operations staff	9%	10%
IT software engineer/developer	10%	10%
IT systems analyst/programmer/engineer	9%	10%
IT vice president	1%	2%
Line of business director	1%	3%
Line of business manager/supervisor	4%	3%
Line of business staff	4%	5%
Line of business vice president	2%	2%
None of the above (stop)	0%	0%
Total	100%	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**	FY2020	FY2019
Q1a. My organization has no difficulty **attracting** qualified candidates.	27%	28%
Q1b. My organization has no difficulty **retaining** qualified candidates.	25%	29%
Q1c. My organization's IT security function is typically understaffed.	69%	75%
Q1d. My company's use of cyber automation will reduce its need for skilled IT security personnel.	24%	28%
Q1e. Human involvement in security is important in the age of automation.	68%	68%

Q2a. What knowledge should an entry-level job candidate have? Please select all that apply.	FY2020	FY2019
Background in data loss prevention	14%	13%
Experience with intrusion prevention and detection systems	20%	20%
Familiarity with security regulations and standards	27%	25%
Knowledgeable about how to provide timely and relevant security reports	19%	19%
Network and system administration experience	25%	18%
Understanding how to communicate to C-level executives and board members	8%	6%
Understanding information security frameworks	26%	24%
Understanding of potential cybersecurity threats	41%	39%
Other (please specify)	4%	1%
Total	184%	164%

Q2b. What knowledge should a highly-experienced (at or above the supervisory level) job candidate have? Please select all that apply.	FY2020	FY2019
Background in data loss prevention	58%	53%
Experience with intrusion prevention and detection systems	75%	84%
Familiarity with security regulations and standards	81%	78%
Knowledgeable about how to provide timely and relevant security reports	63%	68%
Network and system administration experience	56%	61%
Understanding how to communicate to C-level executives and board members	52%	48%
Understanding information security frameworks	78%	79%
Understanding of potential cybersecurity threats	80%	84%
Other (please specify)	6%	4%
Total	549%	559%

Q3a. What IT security technical skills should an entry-level job candidate have? Please select all that apply.	FY2020	FY2019
Create, modify and update intrusion detection systems (IDS)	10%	8%
Create, modify and update security information event management (SIEM) systems	6%	6%
Discover vulnerabilities in information systems	17%	16%
Evaluate and deconstruct malware software	27%	24%
Install firewall and data encryption programs	15%	17%
Maintain security records of monitoring and incident response activities	29%	28%
Monitor compliance with security regulations	17%	12%
Perform cyber and technical threat analyses	23%	19%
Prevent hacker intrusion	17%	17%
Produce situational and incident-related reports	7%	5%
Gathering, processing and managing threat intelligence	23%	
Remediate security issues	10%	10%
Respond to requests for specialized cyber threat reports	14%	8%
Use big data analytics to pinpoint security threats	8%	6%
Other (please specify)	4%	5%
Total	226%	181%

Q3b. What IT security technical skills should a highly-experienced (at or above supervisory level) job candidate have? Please select all that apply..	FY2020	FY2019
Create, modify and update intrusion detection systems (IDS)	61%	61%
Create, modify and update security information event management (SIEM) systems	52%	51%
Discover vulnerabilities in information systems	71%	67%
Evaluate and deconstruct malware software	50%	51%
Install firewall and data encryption programs	45%	43%
Maintain security records of monitoring and incident response activities	52%	52%
Monitor compliance with security regulations	41%	45%
Perform cyber and technical threat analyses	77%	72%
Prevent hacker intrusion	57%	62%
Produce situational and incident-related reports	42%	43%
Gathering, processing and managing threat intelligence	59%	0%
Remediate security issues	73%	72%
Respond to requests for specialized cyber threat reports	64%	66%
Use big data analytics to pinpoint security threats	37%	37%
Other (please specify)	6%	5%
Total	786%	728%

Q4a. Does your organization invest in training/onboarding security personnel?	FY2020	FY2019
Yes	53%	53%
No	47%	47%
Total	100%	100%

Q4b. If yes, how many days does the training/onboarding take?	FY2020	FY2019
Less than 1 day	34%	37%
1 day	29%	27%
2 to 3 days	19%	20%
4 to 5 days	11%	9%
1 week	5%	4%
More than 1 week	3%	3%
Total	100%	100%
Extrapolated value	2.02	1.93

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

Q5a. Does your organization use automation?	FY2020	FY2019
Yes, currently	31%	31%
No, but planning to in the next six to 12 months	36%	39%
No, but planning to within the next three years	10%	10%
We do not plan to use automation	24%	21%
Total	100%	100%

Q5b. If no, why are you not adopting automation? Please select all that apply.	FY2020	FY2019
Automation tools we need are not available	25%	21%
There is a heavy reliance on legacy IT environments	53%	52%
There are Interoperability issues among automation technologies	46%	44%
Lack of budget	47%	49%
Lack of in-house expertise	53%	54%
Lack of C-level support	15%	18%
Other (please specify)	3%	1%
Total	242%	239%

Q6. If yes, what percentage of IT security tasks have been automated?	FY2020	FY2019
1% to 10%	14%	10%
11% to 25%	32%	33%
26% to 50%	35%	40%
51% to 75%	17%	15%
76% to 100%	2%	2%
Total	100%	100%
Extrapolated value	32%	32%

	FY2020	FY2019
Q7a. The inability to properly staff skilled security personnel has increased my company's investment in cyber automation tools and technologies. Strongly agree and Agree response	48%	48%
Q7b. Automation is helping to reduce the stress of our organization's IT security personnel. Strongly agree and Agree response	60%	

Q8. What activities currently performed by your IT security staff are most commonly automated? Please select all that apply.	FY2020	FY2019
Breach and attack simulation	11%	10%
DevOps	15%	14%
IDS/IPS	24%	25%
Incident response	27%	26%
Log analysis	50%	50%
Malware analysis	53%	51%
Provisioning of resources	17%	16%
Pen testing	43%	0%
Responding to requests for cyber threat reports	24%	24%
Threat hunting	40%	38%
Vulnerability scanning	32%	31%
Other (please specify)	2%	2%
Threat intelligence	41%	41%
Total	378%	329%

Q9. 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.	FY2020	FY2019
Breach and attack simulation	15%	14%
DevOps	37%	29%
IDS/IPS	30%	25%
Incident response	40%	38%
Log analysis	68%	67%
Malware analysis	57%	56%
Provisioning of resources	18%	17%
Pen testing	47%	0%
Responding to requests for cyber threat reports	30%	29%
Threat hunting	60%	58%
Threat intelligence	38%	36%
Vulnerability scanning	35%	36%
Other (please specify)	5%	4%
Total	480%	409%

Q10. Which of the following security technologies does your organization fully automate? Please select all that apply.	FY2020
Advanced breach detection	40%
Advanced security/threat analytics and anomaly detection	43%
Advanced testing attack simulation	40%
Antivirus	64%
Cloud application security management	40%
eGRC	32%
Endpoint detection and response (EDR)	54%
Endpoint protection with both EDR and extensible provisioning protocol (EPP) in one package	30%
External threat intelligence platform (not just a data feed)	37%
Messaging security gateway/spam/phishing detection	38%
Network admission control	35%
Next-generation firewall	32%
Orchestration	39%
Machine learning	30%
SIEM	41%
User awareness training such as anti-phishing and cybersecurity awareness	48%
VPN appliances	43%
Vulnerability management	37%
WAF	42%
Web security gateway	40%
Other (Please specify)	4%
Total	809%

Q11. What are the primary benefits of automation? Please select your top four choices.	FY2020	FY2019
Accelerates the containment of infected endpoints/devices/hosts	37%	31%
Decreases the cost of cybersecurity operations	23%	19%
Identifies application security vulnerabilities	25%	29%
Improves the ability to prioritize threats and vulnerabilities	39%	48%
Increases the productivity of current security personnel	43%	46%
Increases the speed of analyzing threats	42%	45%
Provides more in-depth knowledge about security threats	30%	31%
Reduces the complexity of the cyber security architecture	22%	24%
Reduces the false positive and/or false negative rates	43%	41%
Reduces the headcount of IT security personnel	31%	34%
Reduces the manual updating of firewall rules and security policies	30%	30%
Reduces the number of insecure or non-compliant endpoints or things	19%	11%
Reduces the number of security events that must be investigated	13%	11%
Other (please specify)	3%	1%
Total	400%	400%

Q12. What factors in the global business and security landscape influence your organization's use of automation? Please select all that apply.	FY2020	FY2019
New global regulatory compliance standards such as EU GDPR, China Internet Security Law, APEC Privacy Framework, etc.	72%	66%
Threats to our organization's unique sensitive data in the global environment	65%	55%
Threats created by operating in the global digital economy	71%	70%
The importance of demonstrating a strong security posture	59%	51%
To prevent downtime or business disruptions from security incidents	82%	80%
To prevent loss of reputation from security incidents	43%	41%
Threats posed by third-party vendors or business partners	45%	0%
Other (please specify)	4%	2%
Total	441%	366%

Q13. How will automation affect the hiring of IT security personnel? Please select only one choice.	FY2020	FY2019
Automation will increase the need to hire people with more advanced technical skills	35%	43%
Automation will reduce the headcount of our IT security function	51%	30%
Automation will have no affect on our hiring and headcount of our IT security function	13%	27%
Other (please specify)	1%	1%
Total	100%	100%

Q14a. Do you personally think you will lose your job because of automation?	FY2020	FY2019
Yes	37%	28%
No	63%	64%
Unsure	0%	7%
Total	100%	100%

Q14b. If yes, when do you think you will lose your job because of automation?	FY2020	FY2019
Less than 1 year	14%	10%
1 to 2 years	20%	31%
3 to 4 years	27%	30%
5 to 6 years	25%	18%
7 to 10 years	10%	8%
More than 10 years	3%	3%
Total	100%	100%
Extrapolated value	3.95	3.54

Q15a. Does automation improve your IT security staff's ability to do their jobs?	FY2020	FY2019
Yes	63%	63%
No	34%	26%
Unsure	3%	11%
Total	100%	100%

Q15b. If yes, why? Please select all that apply.	FY2020	FY2019
It enables our IT security staff to focus on more serious vulnerabilities and overall network security	74%	71%
It automates time intensive, manual processes that are mission critical but not a good use of staff time	42%	40%
It will reduce human error	40%	40%
Other (please specify)	5%	7%
Total	160%	157%

Q15c. If it does not improve your IT security staff's ability to do their jobs, why? Please select all that apply.	FY2020	FY2019
Automation will never replace human intuition and hands-on experience	54%	49%
Automation will make jobs more complex	50%	47%
Automation is not able to catch certain threats	45%	35%
Human intervention is necessary for network protection	47%	44%
Automation is not capable of performing certain tasks that the IT security staff can do	74%	68%
Other (please specify)	6%	7%
Total	276%	251%

Q16. Do you see an increase in attackers' use of automation?	FY2020	FY2019
Yes	53%	47%
No	47%	53%
Total	100%	100%

Q17a. Are your organization's CEO and/or board of directors briefed on its use of automation?	FY2020
Yes	40%
No	60%
Total	100%

Q17b. If yes, how often is the CEO and/or board of directors briefed?	FY2020
Monthly	6%
Quarterly	19%
Bi-annually	18%
Annually	21%
No formal schedule	20%
Only when our organization has a security incident	16%
Total	100%

Q17c. If yes, are any of the following metrics reported to the CEO and/or board of directors? Please select all that apply.	FY2020
Decrease in the cost of cybersecurity operations	30%
Improvement in the ability to prioritize threats and vulnerabilities	38%
Improvement in the productivity of IT security personnel	43%
Retention of in-house expert personnel	37%
Decrease in false positives and/or false negative rates	54%
Decrease in the headcount of IT security personnel	33%
Decrease in the number of security events that must be investigated	39%
Other (Please specify)	4%
Total	277%

Part 4. General IT security questions

Q18. Which of the following security technologies does your organization deploy? Please select all that apply.	FY2020	FY2019
Advanced breach detection	39%	39%
Advanced security/threat analytics and anomaly detection	47%	44%
Advanced testing attack simulation	23%	27%
Antivirus	87%	87%
Cloud application security management	46%	38%
eGRC	55%	53%
Endpoint detection and response (EDR)	52%	52%
Endpoint protection with both EDR and extensible provisioning protocol (EPP) in one package	30%	32%
External threat intelligence platform (not just a data feed)	44%	37%
Messaging security gateway/spam/phishing detection	43%	37%
Network admission control	33%	34%
Next-generation firewall	53%	48%
Orchestration	37%	0%
Machine learning	39%	0%
Security automation and orchestration	41%	41%
Security policy orchestration and automation	33%	39%
SIEM	50%	46%
Threat intelligence platform	43%	39%
User awareness training such as anti-phishing and cybersecurity awareness	50%	50%
VPN appliances	38%	41%
Vulnerability management	42%	40%
WAF	48%	48%
Web security gateway	34%	37%
Other (please specify)	2%	2%
Average number of deployed security technologies	10.08	9.09

Q19. Does your organization have a security operations center (SOC)?	FY2020	FY2019
Yes	61%	58%
No	39%	42%
Total	100%	100%

Q20. On average, how many security incidents/tickets does the security team receive **per day**?	FY2020	FY2019
Less than 25	1%	2%
26 to 50	5%	6%
51 to 100	10%	16%
101 to 250	15%	22%
251 to 500	35%	28%
501 to 1,000	22%	15%
More than 1,000	11%	12%
Total	100%	100%
Extrapolated value	468	407

Q21. On average, how many severe/critical security incidents/tickets does the security team receive **per day**?	FY2020	FY2019
Less than 25	14%	11%
26 to 50	24%	24%
51 to 100	31%	31%
101 to 250	19%	22%
251 to 500	7%	6%
501 to 1,000	4%	5%
More than 1,000	1%	2%
Total	100%	100%
Extrapolated value	137	149

Q22. Approximately how many staff hours does your organization spend investigating or triaging alerts **per day**?	FY2020	FY2019
1 to 4	1%	
5 to 8	5%	
9 to 24	14%	
25 to 40	28%	
41 to 80	28%	
81+	24%	
Total	100%	
Extrapolated value	63.5	61

*Scale changed in FY 2020

Q23. Which of the following are integrated with your organization's security management tools? Please select all that apply.	FY2020	FY2019
Advanced IT analytics	24%	19%
Application dependency mapping	16%	12%
Application performance management	19%	14%
Change management	32%	30%
Cloud services analytics	19%	15%
CMDP	25%	24%
Cross-domain operations	18%	22%
Directory services	49%	43%
End user experience monitoring	51%	50%
Event management	46%	44%
Help desk	40%	40%
Orchestration	35%	32%
Security monitoring	54%	51%
Virtual systems management	40%	36%
Other (please specify)	4%	1%
Total	472%	435%

Q24. Does your organization use threat intelligence in its cybersecurity program?	FY2020
Yes	48%
No	52%
Total	100%

Q25. Does your organization have resources that focus on threat detection?	FY2020
Yes, single dedicated person	18%
Yes, formal dedicated team	19%
Yes, shared responsibility across multiple security groups	24%
No, but we plan to	11%
No, we don't plan to	28%
Total	100%

Q26. If yes, what threat intelligence data does your organization consume? Please select all that apply.	FY2020
DNS traffic	28%
Web and email filter data	49%
Network traffic	69%
Firewall/IPS traffic	62%
Server traffic	54%
Packet sniff/tcp dump	41%
File monitoring data	30%
User behavior	40%
Endpoint activity	58%
Active directory	42%
Access/authentication logs	34%
System log	52%
Threat intelligence sources	60%
Web proxy logs	33%
Dark web data	44%
Social media	43%
Other	4%
Total	743%

Q27a Does your organization share threat intelligence with other organizations?	FY2020
Yes	48%
No	52%
Total	100%

Q27b. If yes, what are the benefits of sharing intelligence with other groups? Please select all that apply.	FY2020
Learn about threats affecting organizations similar to us	41%
Ability to collaborate with industry peers about known active threats	53%
Ability to proactively monitor for threats seen by peers	43%
Ability to integrate knowledge from peers into our organization's threat detection tools	40%
Other	7%
Total	183%

Q27c. If no, why doesn't your organization share threat intelligence with other organizations? Please select all that apply.	FY2020
Nothing of value to share	44%
Concerns about the privacy of our corporate data	36%
Concerns about corporate liability	31%
Concerns about the potential for misuse of the data	52%
Lack of expertise in threat intelligence	66%
Concerns about revealing a possible data breach	33%
Concerns about GDPR exposure	25%
Other	4%
Total	292%

Part 5. Your role and organization

D1. Experience	FY2020	FY2019
Total years of relevant experience	9.28	8.81
Total years in current position	6.47	6.14

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	FY2020	FY2019
CEO/executive committee	4%	3%
Chief operating officer	2%	1%
Chief information officer	47%	42%
Chief technology officer	8%	9%
Chief financial officer	0%	0%
Leader, human resources	0%	1%
Leader, business unit or LOB	11%	10%
Leader, corporate compliance	5%	2%
Leader, risk management	5%	8%
Leader, IT administration	0%	1%
Data center management	2%	2%
Chief security officer	2%	2%
Chief information security officer	15%	19%
Total	100%	100%

D3. What industry best describes your organization's primary sector?	FY2020	FY2019
Agriculture & food services	1%	1%
Communications	3%	3%
Consumer products	5%	6%
Defense & aerospace	1%	1%
Education & research	1%	1%
Energy & utilities	6%	5%
Entertainment & media	1%	0%
Financial services	17%	18%
Health & pharmaceutical	9%	10%
Hospitality	1%	1%
Industrial/manufacturing	12%	11%
Public sector	11%	10%
Retail	8%	9%
Services	11%	11%
Technology & software	8%	9%
Transportation	4%	4%
Other	1%	1%
Total	100%	100%

D4. What best describes your organization's geographic footprint?	FY2020	FY2019
Domestic	17%	15%
Primarily one global region	26%	22%
Primarily two or more global regions	29%	35%
All global regions (multinational)	28%	28%
Total	100%	100%

D5. What is the worldwide headcount of your organization?	FY2020	FY2019
Less than 1,000	14%	14%
1,000 to 5,000	26%	25%
5,001 to 10,000	25%	27%
10,001 to 25,000	20%	18%
25,001 to 75,000	9%	10%
More than 75,000	6%	6%
Total	100%	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.