The Economics of Security Operations Centers: What is the True Cost for Effective Results?

Sponsored by Respond Software

Independently conducted by Ponemon Institute LLC

Publication Date: January 2020

The Economics of Security Operations Centers: What Is the True Cost for Effective Results?

Presented by Ponemon Institute, January 2020

Part 1. Executive summary

Ponemon Institute is pleased to present the findings on the economics of today's Security Operations Centers (SOC). Sponsored by Respond Software, Ponemon Institute surveyed 637 IT and IT security practitioners in organizations that have a SOC and are knowledgeable about cybersecurity practices in their organizations. Respondents supervise or are responsible for such activities as information security, threat detection and remediation and security operations management and more.

Results and analysis of the findings offer new insights into the economics and effectiveness of SOCs. At the forefront are challenges from a return on investment (ROI) perspective. According to the research, a majority of surveyed organizations find their investments in SOCs to be expensive and yield mediocre results.

On average, organizations spend $2.86 million annually on their in-house SOC. Surprisingly, the cost significantly increases to $4.44 million annually if they outsource to a managed security service provider (MSSP), negating cost efficiency expectations from outsourcing. Despite this significant investment, only slightly more than half of organizations represented (51 percent) in this study are satisfied with the effectiveness of their SOC in detecting attacks.

The study found most companies view their SOCs as a crucial element of their cybersecurity strategies, especially for minimizing false positives and reporting threat intelligence information. To be effective, SOCs rely upon the expertise of individuals to prevent, detect, analyze and respond to cybersecurity incidents. However, such expertise can be costly in terms of salaries, turnover and the training of analysts.

The study also reflects the substantial impact and cost of personnel for SOCs. The expense to hire, train and retain employees is high and increasing, and turnover is rampant. Interestingly, while the best performing SOCs have a greater number of employees and slightly less turnover, they cost significantly more, and most organizations can't or don't have the resources to build out that infrastructure. Thus, organizations turn to outsourcing, but only 17 percent of respondents find their MSSPs to be highly effective.

The following findings illustrate the typical SOC's true cost

- The salary of the average analyst is $102,315 and 45 percent of respondents say salaries are expected to increase an average of 29 percent in 2020.
- The time to hire and train one analyst is almost one year and on average the analyst stays slightly more than two years.
- The cost effectiveness of the SOC is diminished because those responsible for hiring and training say it takes them away from their other responsibilities.
- The cost of a SOC is higher if the IT infrastructure it monitors is on-premise or mobile.
- Financial services spend significantly more on their SOC than other industries.
- An effective SOC costs more. SOCs that are highly effective cost an average of $3.5 million versus $1.96 million if the SOC has very low effectiveness.

- The higher the headcount, the costlier the SOC is to maintain. Companies with a headcount of between 25,000 and 75,000 spend an average of $6.27 million versus companies with a headcount of less than 5,000 spend an average of $1.68 million.

This study highlighted many of the challenges and perceptions regarding SOCs. The next two sections provide analysis and key findings, detailed responses, and study methods.

Part 2. Key findings

In this section of the report, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix. We have organized the report according to the following themes.

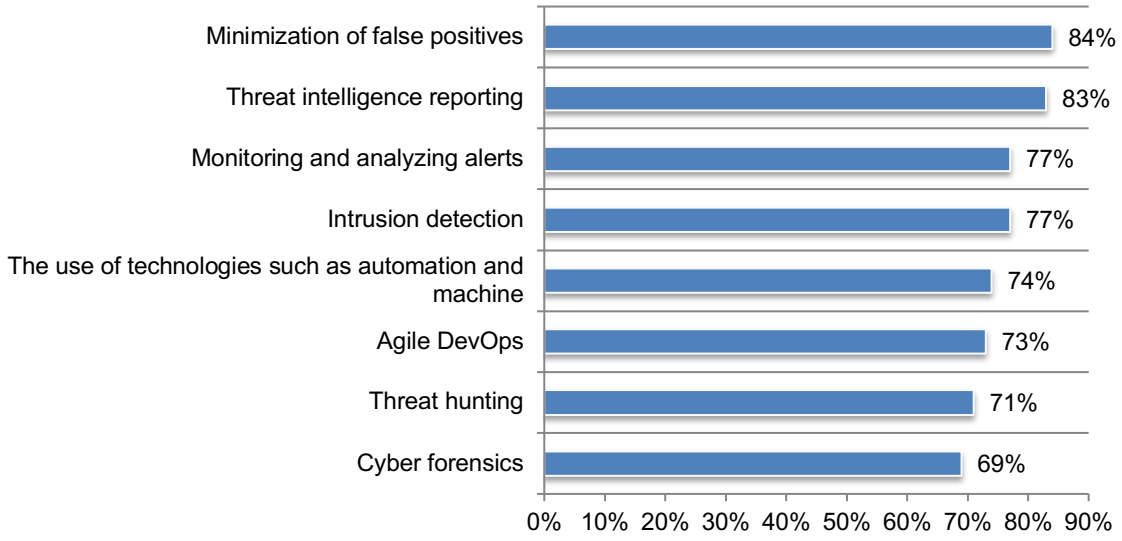
- The state of today's SOC
- Staffing the SOC is costly and challenging
- What impacts the cost of an internal SOC
- Cost considerations when outsourcing the SOC
- ROI considerations of high performing SOCs

The state of today's SOC

SOCs are considered critical in detecting attacks and are core to most cybersecurity strategies. Seventy-three percent of respondents say their SOCs are essential (31 percent) or very important (42 percent) to their overall cybersecurity strategy.

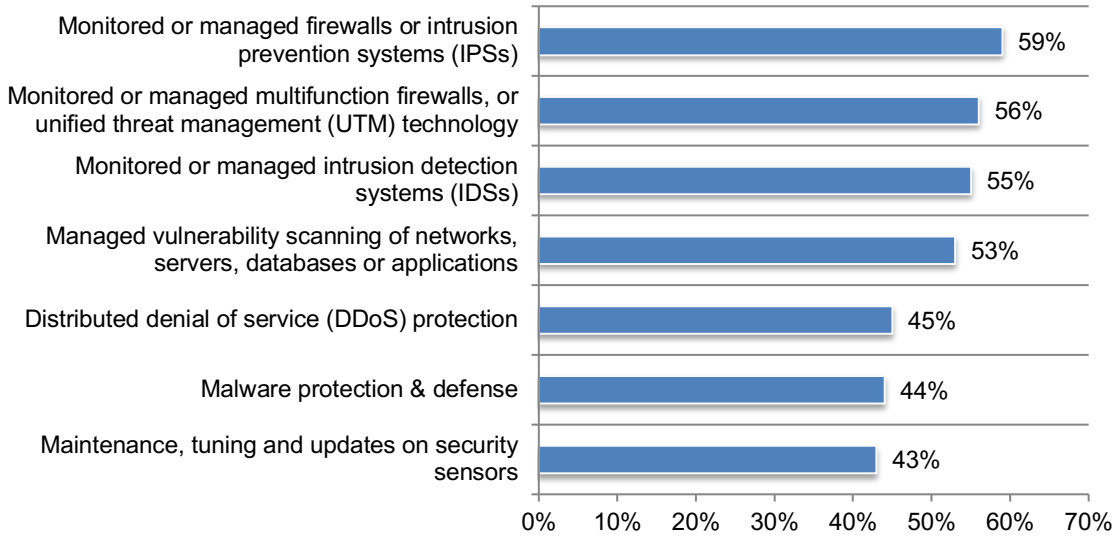
As shown in Figure 1, the most important SOC activities are to minimize false positives and threat intelligence reporting. Respondents were asked to rate the importance of SOC activities from 1 = not important to 10 = very important. While all SOC activities listed in Figure 1 are considered very important by most respondents, the most important are minimization of false positives (84 percent of respondents) and threat intelligence reporting (83 percent of respondents).

Figure 1. The importance of SOC activities
On a scale of 1 = low importance to 10 = high importance, 7+ responses presented



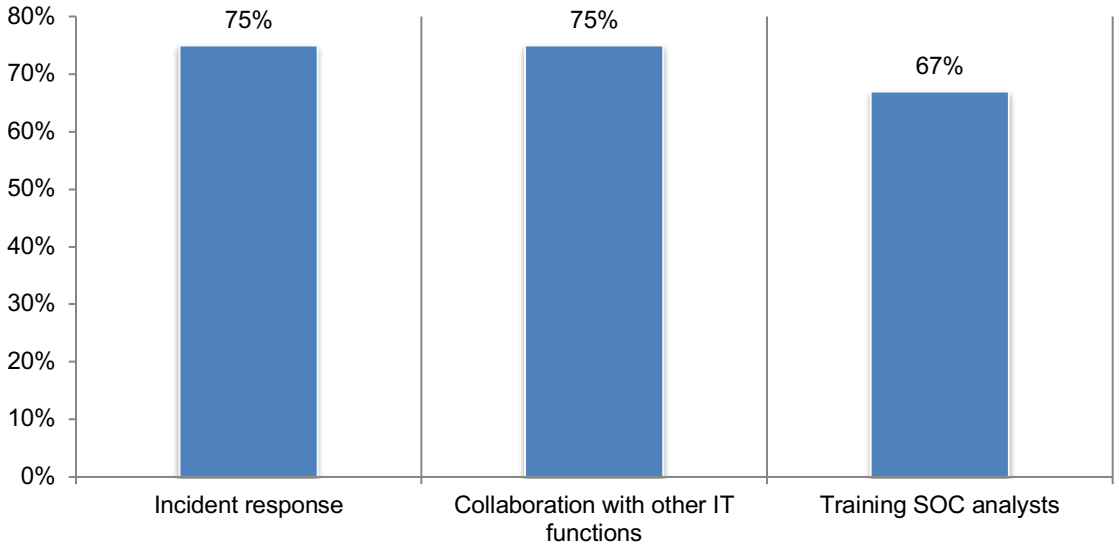
The top SOC services monitor and manage firewalls, IPSs and IDSs. Figure 2 lists the top seven core services typically deployed in organizations represented in this research. The majority of respondents say their SOC monitors or manage firewalls or intrusion prevention systems (IPSs), multifunction or unified threat management (UTM) technology, or intrusion detection systems (IDSs). Fifty-three percent of respondents say vulnerability scanning of networks, servers, databases or applications in the SOC.

Figure 2. The top seven core services typically deployed within the SOC environment
More than one response permitted



Training SOC analysts is ranked as one of the most important SOC activities. Sixty-seven percent of respondents say training of SOC analysts is highly important, as shown in Figure 3. Other highly rated activities are incident response and collaboration with other IT functions (75 percent of respondents).

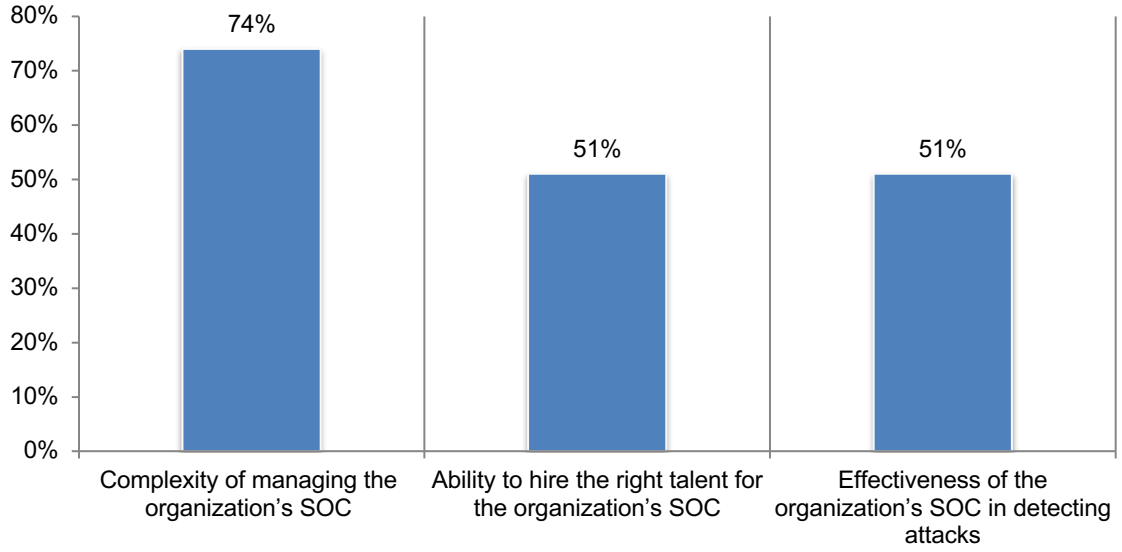
Figure 3. The importance of SOC activities
On a scale of 1 = low importance to 10 = high importance, 7+ responses presented



Staffing the SOC is costly and challenging

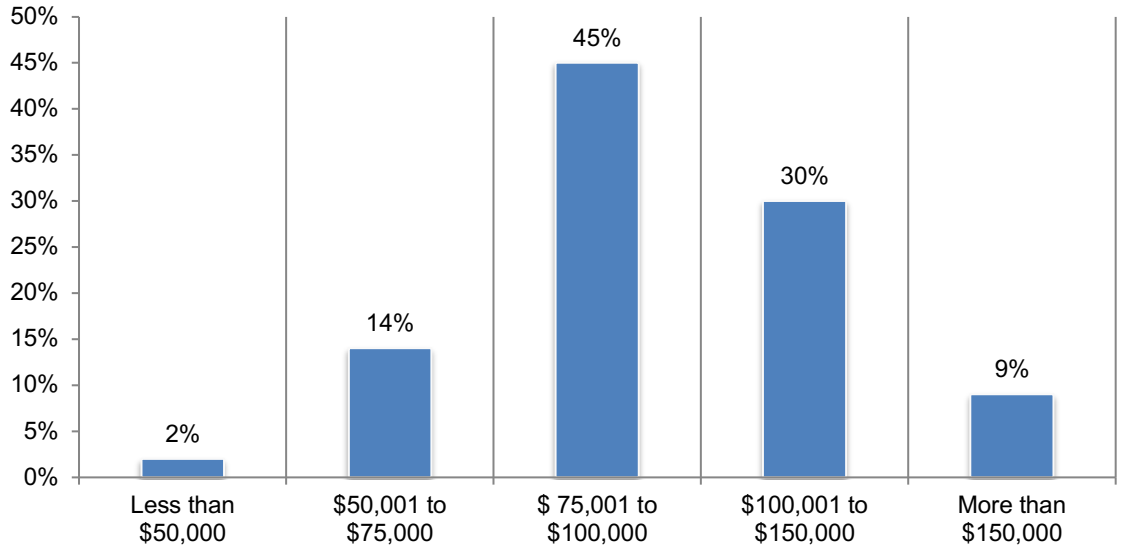
Complexity and the inability to hire the right talent reduces the effectiveness of the SOC's ability to detect attacks. Respondents were asked to rate the complexity of managing the SOC on a scale from 1 = low complexity to 10 = high complexity and the effectiveness in detecting attacks on a scale from 1 = low effectiveness to 10 = high effectiveness. As shown in Figure 4, 74 percent of respondents say their SOCs are highly complex making management difficult. As a result, only about half of respondents (51 percent) say their organizations are highly effective in detecting attacks.

Figure 4. The complexity, effectiveness of SOCs and the ability to hire the right talent
From 1 = low complexity to 10 = high complexity, 7+ responses presented
From 1 = low ability to 10 = high ability
From 1 = low effectiveness to 10 = high effectiveness



Staffing the SOC is costly because of salaries paid and the high turnover of analysts. On average, 12 IT security personnel are assigned to their organization's SOC. According to Figure 5, the average salary for a tier one analyst is $102,315. Forty-five percent of respondents say salaries are expected to increase an average of 29 percent in 2020.

Figure 5. What is the average salary for a tier one analyst?
Extrapolated value = $102,315



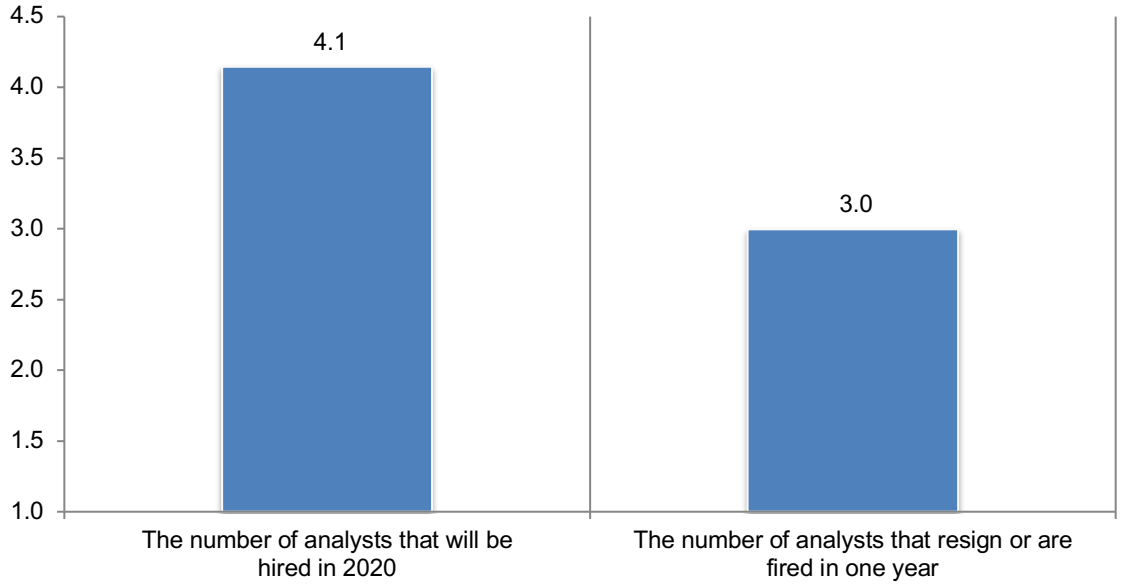
As shown in Figure 6, an analyst leaves the organization in a little more than two years (27.2 months). However, on average almost 8 months is required to find a new analyst (3.5 months) and to train one analyst (3.8 months).

Sixty-five percent of respondents say the time spent hiring and training SOC analysts has a significant impact on the ability for those responsible to complete their other responsibilities.

Figure 6. Turnover and the time spent hiring and training one analyst
Extrapolated values presented

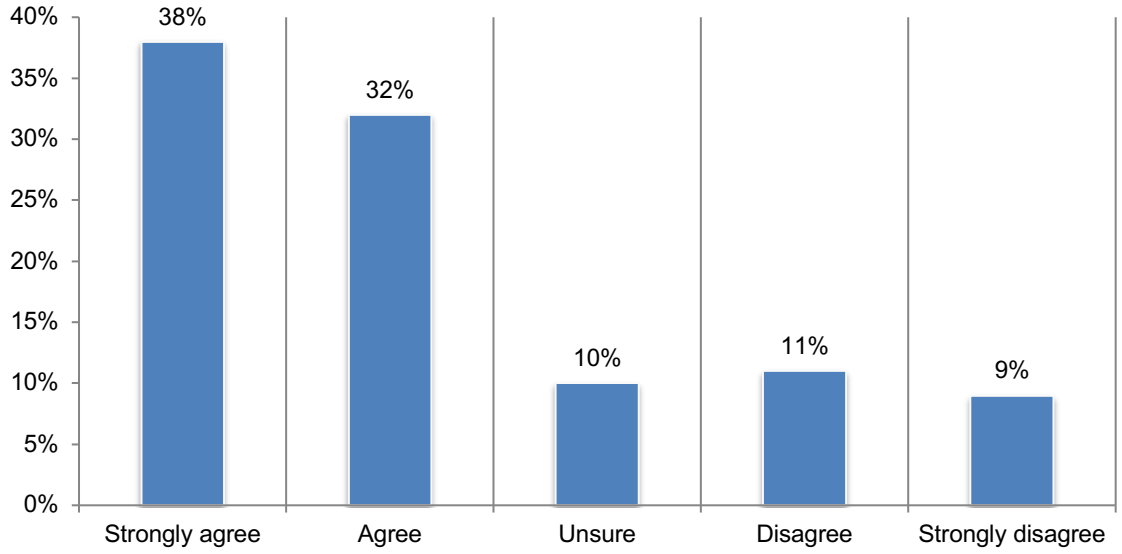
Organizations can't keep pace with turnover. While an average of four analysts are expected to be hired in 2020, as shown in Figure 7, three analysts will be fired or resign in one year.

Figure 7. The hiring and firing of analysts in one year
Extrapolated values presented



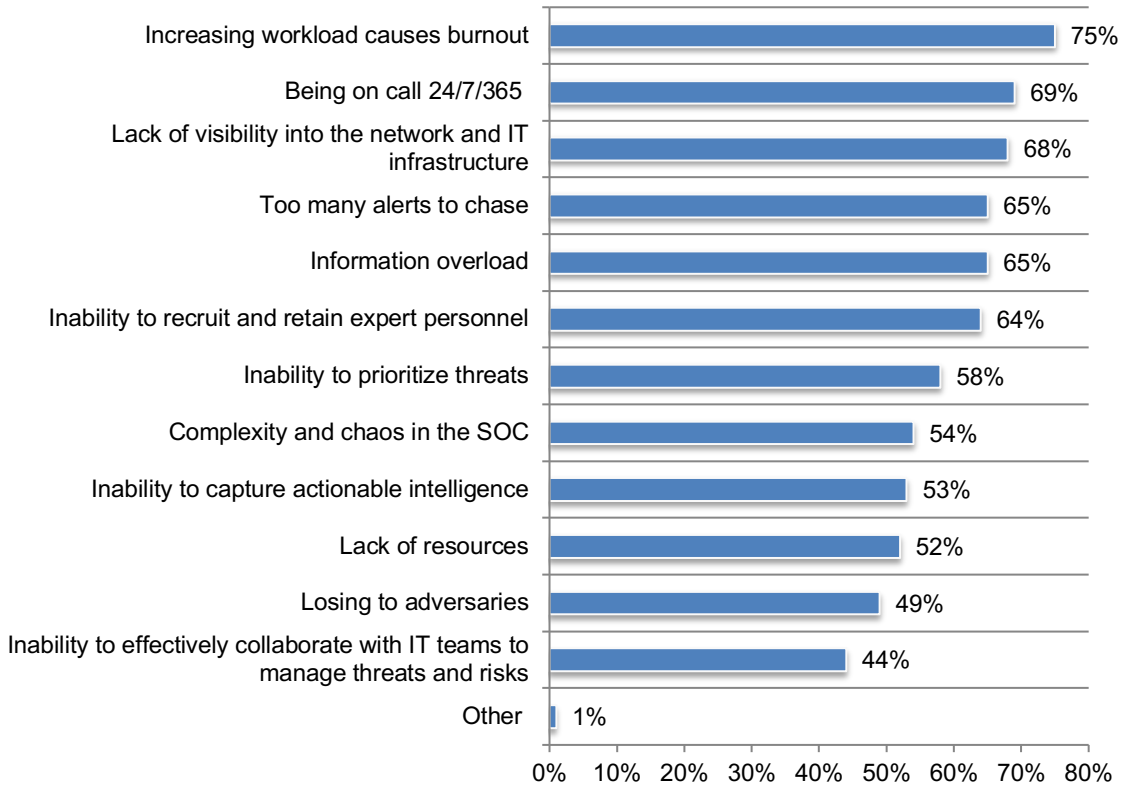
SOC stress is a reason for high turnover. As shown in Figure 8, 70 percent of respondents agree that SOC analysts burn out quickly because of the high-pressure environment and workload.

Figure 8. Our SOC analysts burn out quickly because of the high-pressure environment



Workload and being on call 24/7/365 make working in the SOC painful. As shown in Figure 9, 75 percent of respondents say an increasing workload causes burnout followed by 69 percent of respondents who say it is always having to be on call.

Figure 9. What makes working in the SOC painful?
More than one response permitted



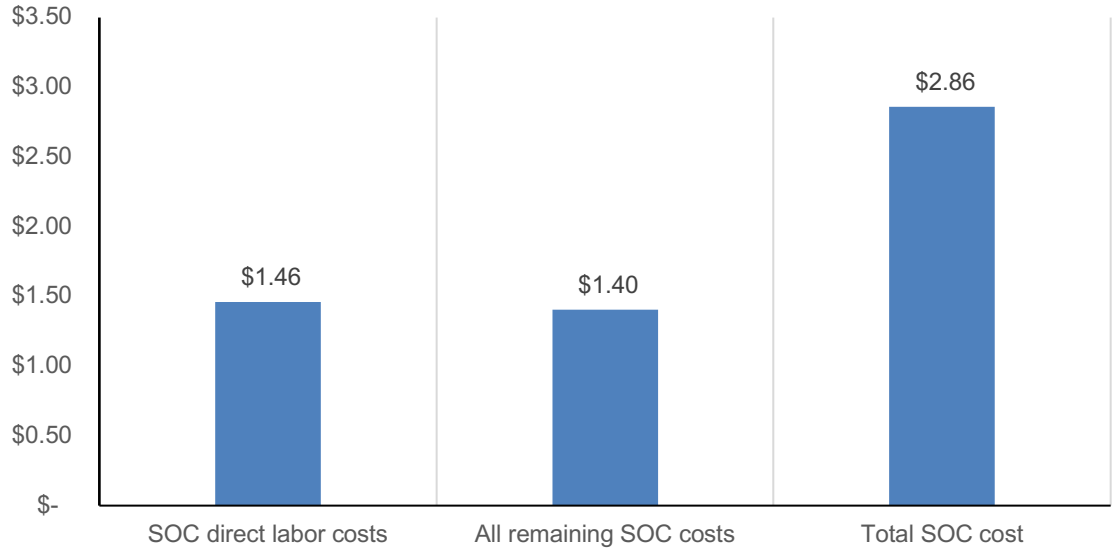
What impacts the cost of a SOC

Fort-four percent of respondents strongly agree (23 percent) or agree (21 percent) that the ROI of their SOC is getting worse. To understand what is impacting the ROI of SOCs, we look at the following five factors:

- The IT infrastructure monitored by the SOC
- Industry
- Complexity of the SOC
- Effectiveness of the SOC in detecting attacks
- Worldwide headcount

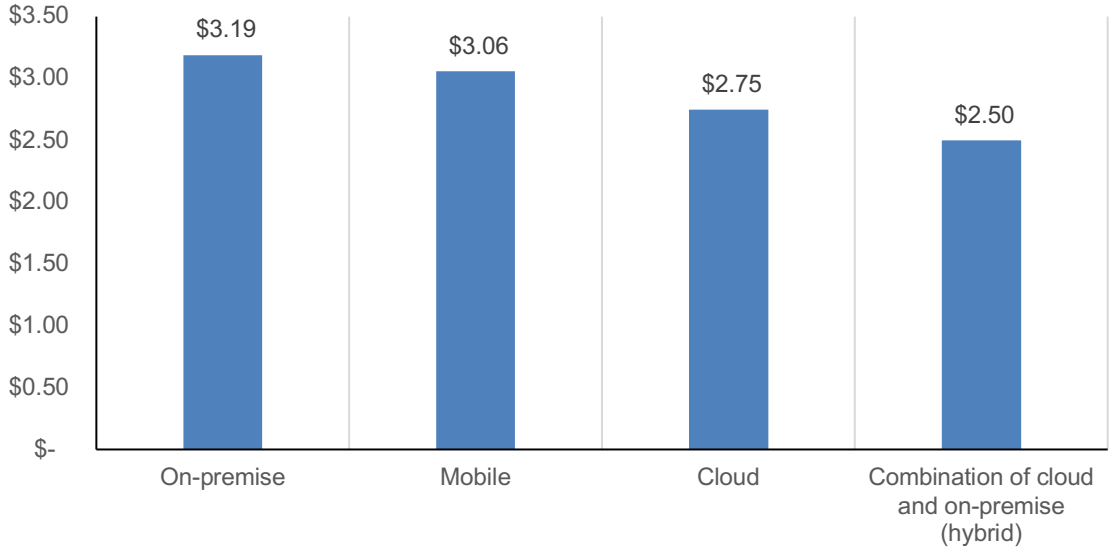
Figure 10 shows the annual average direct labor costs and all remaining SOC costs. On average, organizations are spending almost $3 million annually to support their SOC operations.

Figure 10. Average total cost for maintaining the SOC
US$ millions



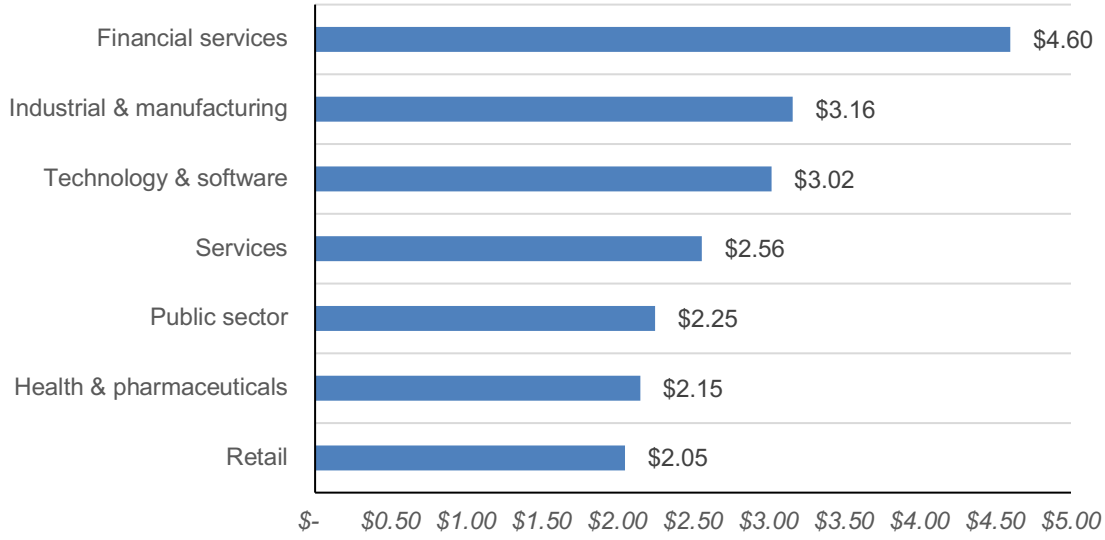
The cost of a SOC is affected by the IT infrastructure monitored by the SOC. As shown in Figure 11, If the IT infrastructure is on-premise or mobile, the average cost is higher.

Figure 11. What best defines the IT infrastructure monitored by your SOC?
US$ million



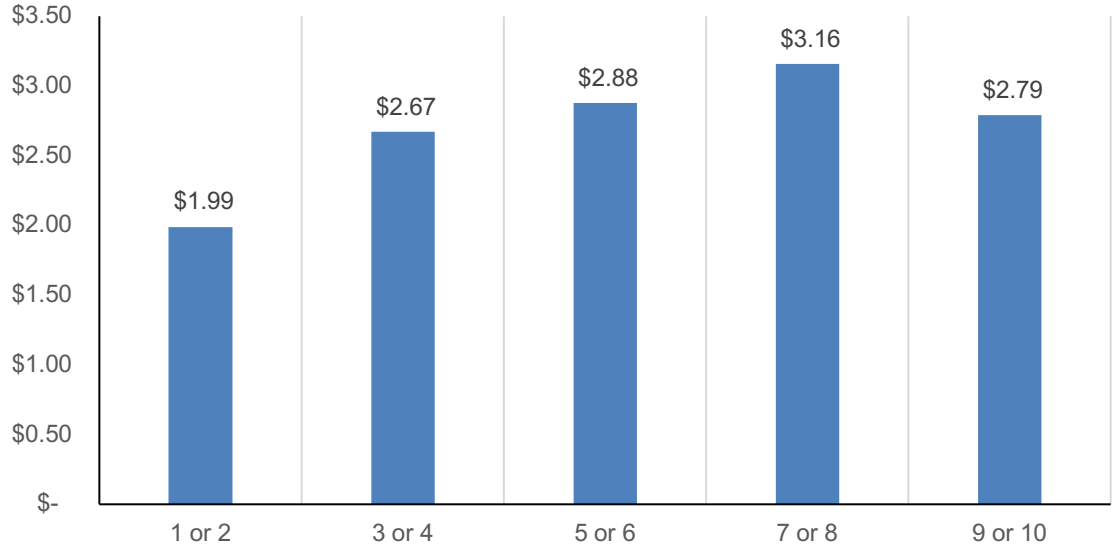
Financial services spend significantly more on their SOCs. As shown in Figure 12, the average cost of SOC in financial services is $4.60 million. SOCs in the retail sector cost the least.

Figure 12. What best describes your organization's industry focus?
US$ million



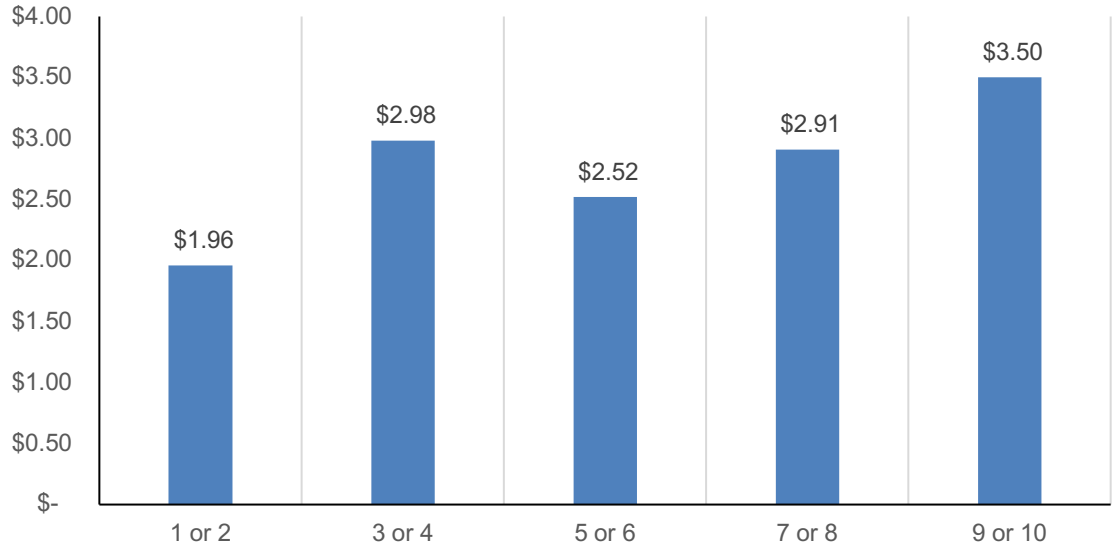
Organizations that rate the complexity of managing their SOC as high (7+ responses) are likely to spend more, as shown in Figure 13.

Figure 13. Rate the complexity of managing your organization's SOC from 1 = low complexity to 10 = high complexity.
US$ millions



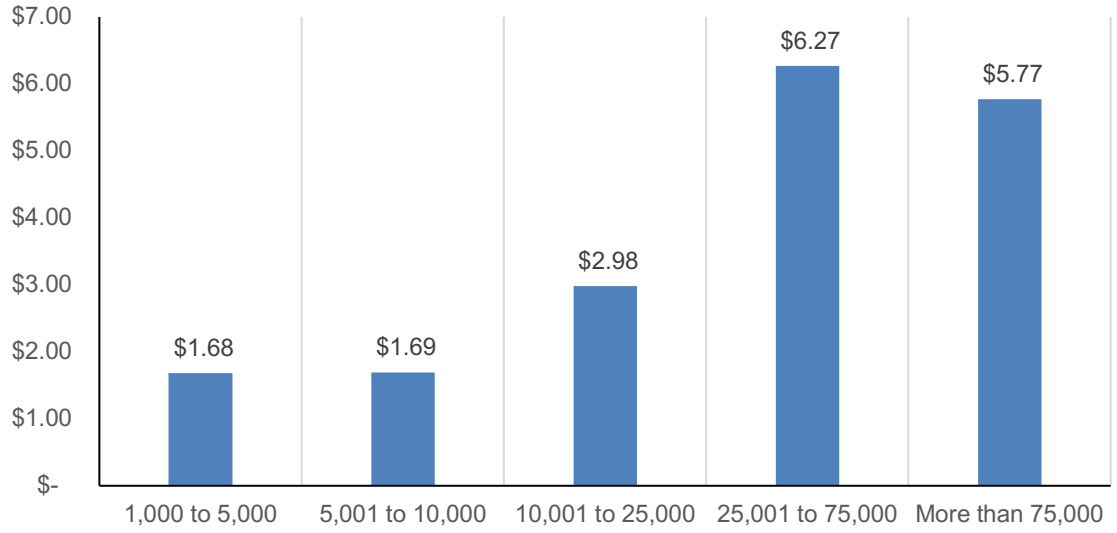
The more effective the SOC, the higher the cost. Respondents were asked to rate the effectiveness of the SOC in detecting attacks. According to Figure 14, respondents who rate their effectiveness as very high (9+ responses) tend to spend more to improve the SOC's ability to detect attacks.

Figure 14. Rate the effectiveness of your organization's SOC in detecting attacks from 1 = low effectiveness to 10 = high effectiveness.
US$ millions



The higher the headcount, the costlier the SOC is to maintain. Figure 15 provides a breakdown of the average cost of a SOC by headcount. However, organizations with a headcount of more than 75,000 spend less than those with a headcount between 25,001 to 75,000. Possibly because of economies of scale.

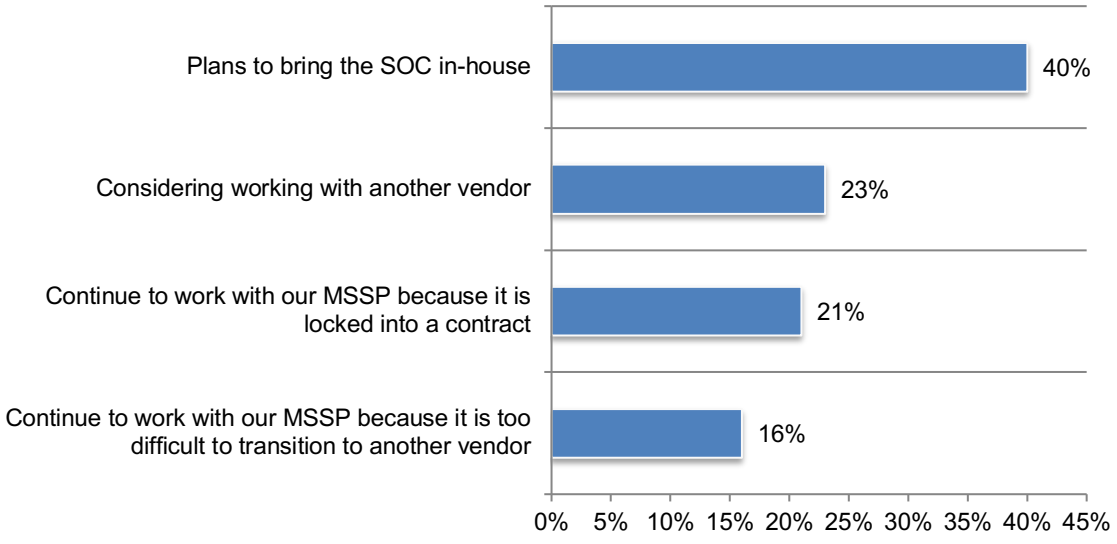
Figure 15. What is the worldwide headcount of your organization
US$ millions



Cost considerations of outsourcing to an MSSP

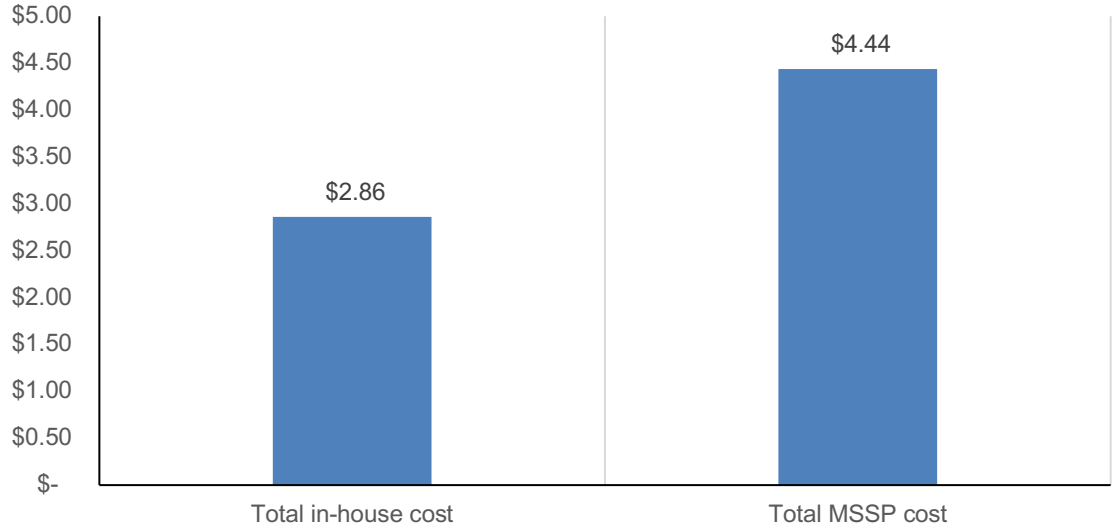
Internal staffing issues provide a good reason to outsource SOC capabilities to an MSSP. Fifty-one percent of respondents say they partially or completely outsource the SOC. Of these respondents, 63 percent of respondents say they will bring their SOC back in-house or switch to another vendor, as shown in Figure 16. However, organizations should shop vendors carefully since 32 percent of respondents say their MSSPs are only moderately effective and 26 percent of respondents say they are ineffective.

Figure 16. If not effective, what actions does your organization plan to take?
More than one response permitted



According to Figure 17, the average annual cost when outsourcing the SOC is $4.44 million, almost double the average cost if the SOC is in-house ($2.86 million). The total cost may be higher or lower depending upon the services the MSSP provides.

Figure 17. In-house SOC versus MSSP extrapolated cost
US$ millions

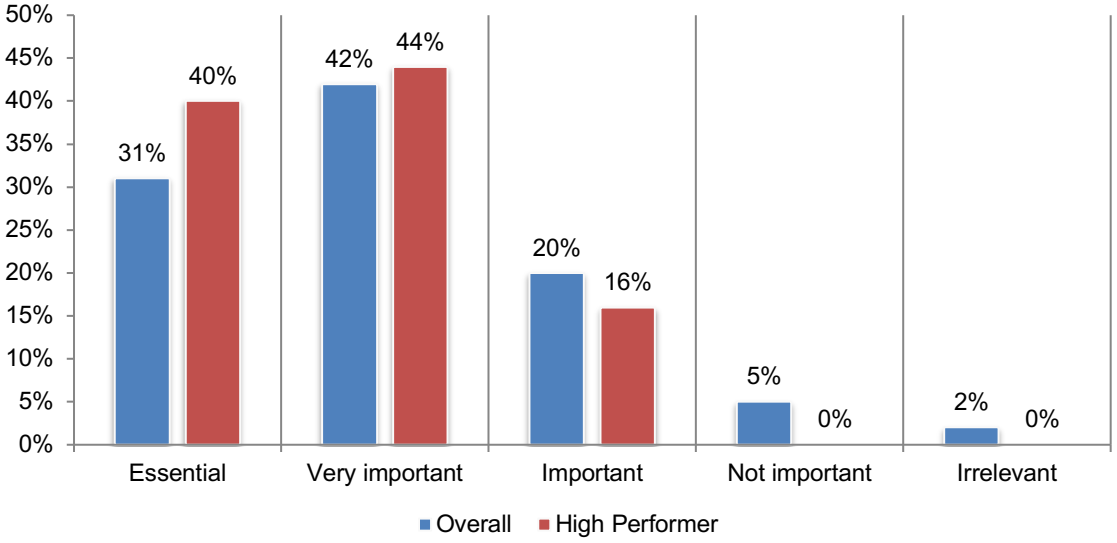


ROI considerations of high performing SOCs

In this section, we analyze the practices of 134 respondents who self-reported that their organization's SOC is highly effective in detecting attacks (9 responses on a scale of 1 = not effective to 10 = highly effective). We refer to the organizations these respondents work in as high performers.

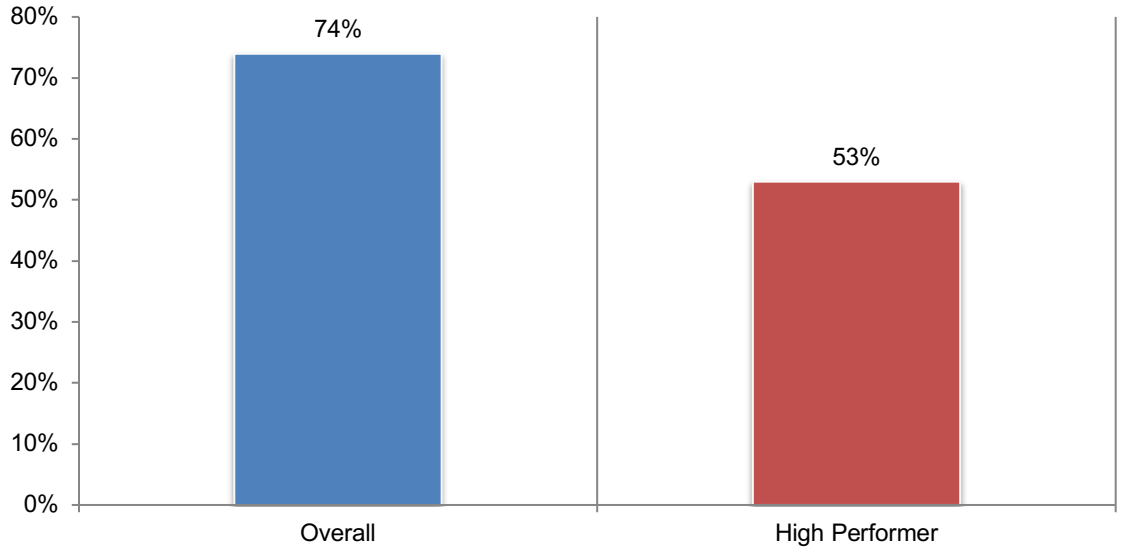
High performers are much more likely to consider their SOC as important to their overall cybersecurity strategy. As shown in Figure 18, 84 percent of high performers versus 73 percent of the overall sample of respondents.

Figure 18. How important is your organization's SOC to its overall cybersecurity strategy?



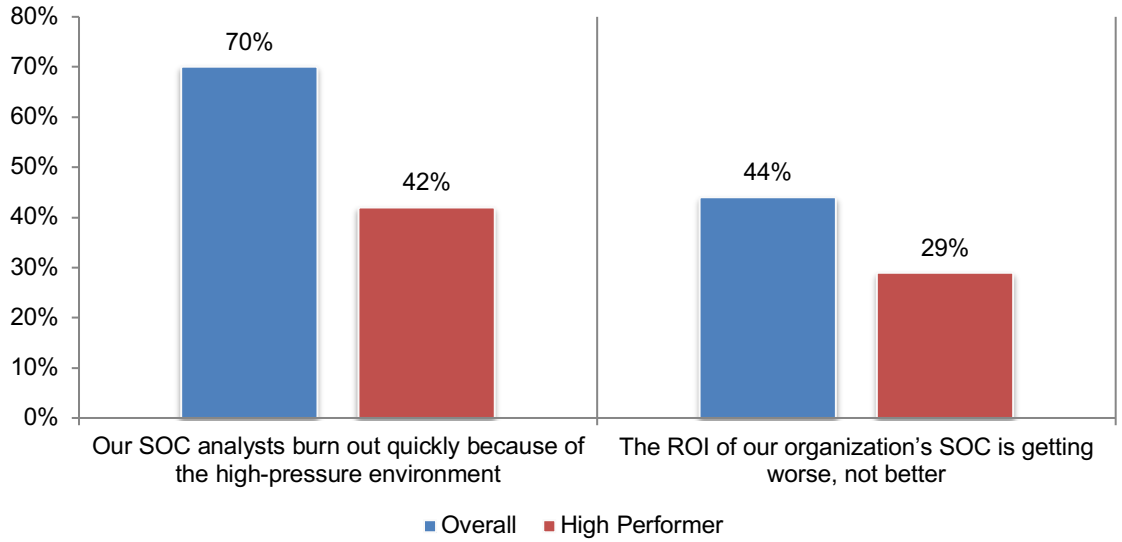
Even though high performers can reduce complexity in the SOC, the majority still say managing a SOC is complex. According to Figure 19, 74 percent of the overall sample say their SOCs are highly complex. In contrast, 53 percent of high performers say their SOCs are highly complex.

Figure 19. How complex is the management of your organization's SOC?
On a scale of 1 = low complexity to 10 = high complexity, 7+ responses



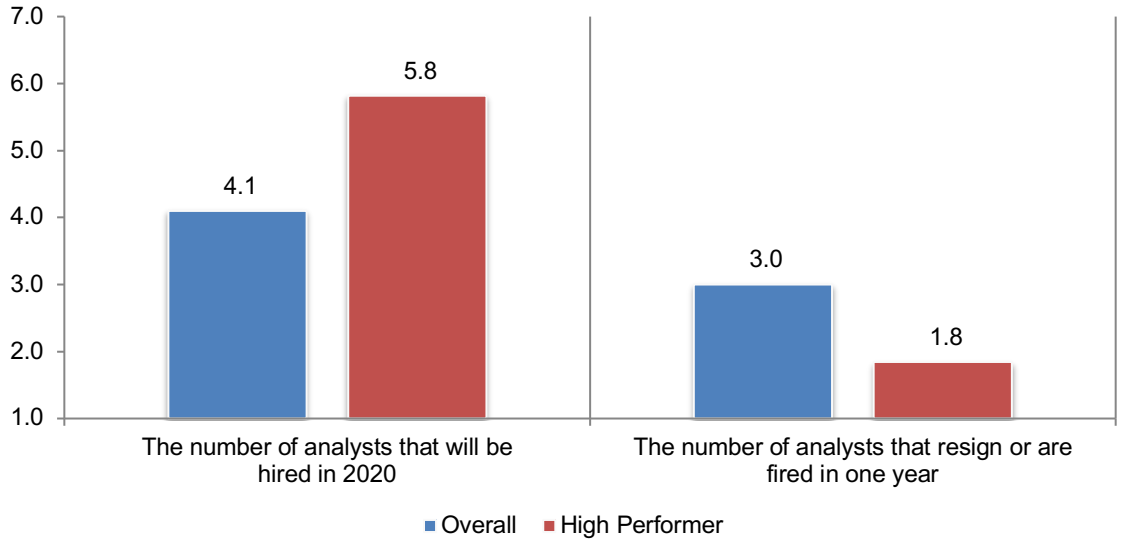
High performers are better at managing analyst burnout and ROI. According to Figure 20, 70 percent of the overall sample say that their SOC analysts burn out quickly because of stress vs. 42 percent of the high performers who report their analysts burn out. Fewer high performers (29 percent vs. 44 percent) say the ROI of their organizations' SOC is getting worse, not better

Figure 20. Perceptions about ROI and staff burnout
Strongly agree and Agree responses combined



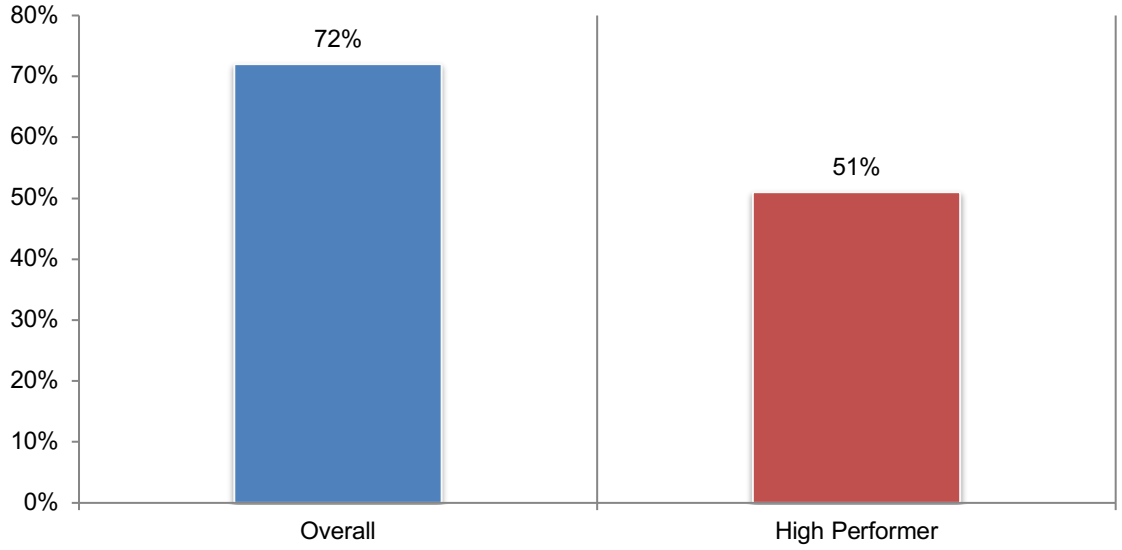
High performers hire more and lose fewer analysts in one year. As shown in Figure 21, high performing organizations are hiring an average of six analysts in one year and an average of two analysts resign or are fired in one year. However, even in high performing organizations attrition is much higher than the overall sample (31 percent vs. 15.1 percent[1]). In the overall sample, an average of four analysts will be hired and three analysts will resign or be fired in one year.

Figure 21. The hiring and firing of analysts in one year
Extrapolated values presented



High performers can improve the pain of working in a SOC, but a majority still report high pain levels. As shown in Figure 22, 72 percent of respondents in the overall sample rate the pain of working in the SOC as very high. Only slightly more than half of high performers rate their pain as very high.

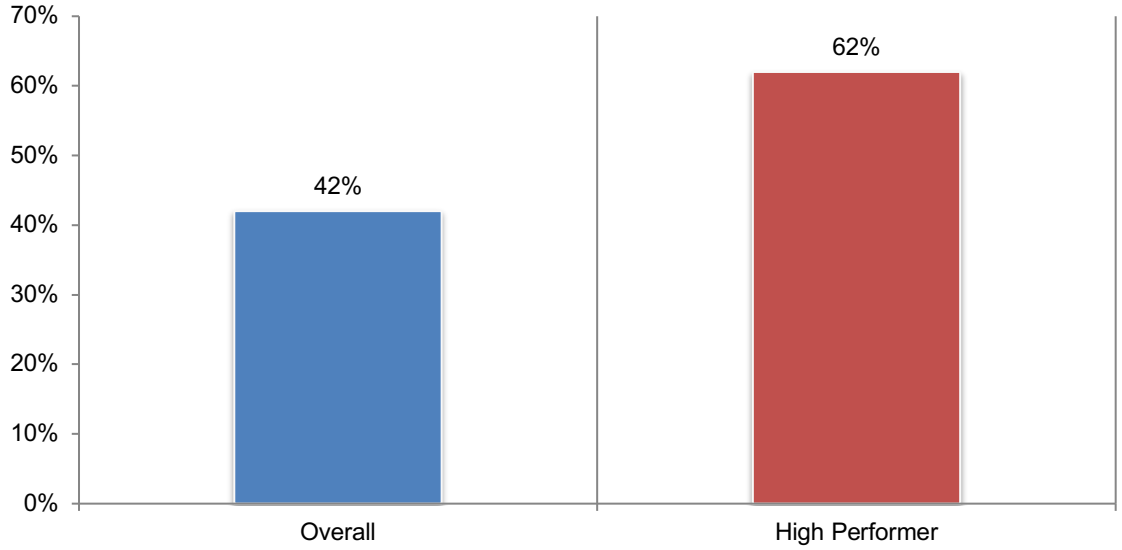
Figure 22. How much pain does your organization's SOC security personnel experience in meeting their daily job requirements
On a scale of 1 = low pain to 10 = high pain, 7+ responses presented



[1] Source: dailypay, July 10,2017

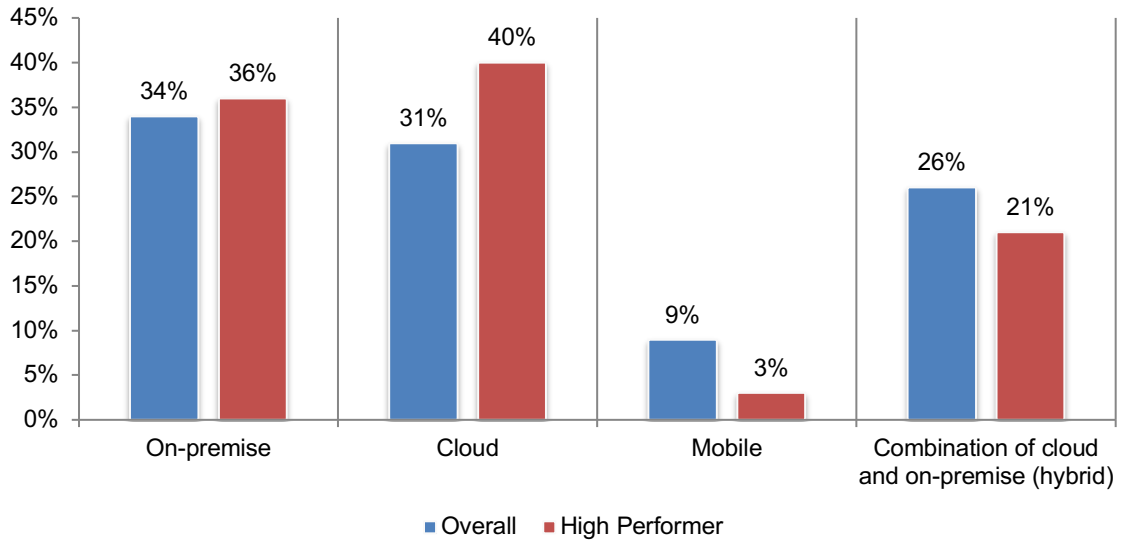
High performers have more effective MSSPs. According to Figure 23, 62 percent of high performing respondents rate the effectiveness of their MSSPs as very high. In contrast, only 42 percent of the overall sample rate the effectiveness of their MSSPs as being very effective.

Figure 23. How effective is your MSSP?
On a scale of 1 = not effective to 10 = very effective, 7+ responses presented



High performers are more likely to have the cloud monitored by their SOC. As shown in Figure 24 40 percent of high performer respondents say the cloud is monitored by their SOC. The overall sample is more likely to have a combination of cloud and on-premise monitored by the SOC.

Figure 24. What best defines the IT infrastructure monitored by your SOC?



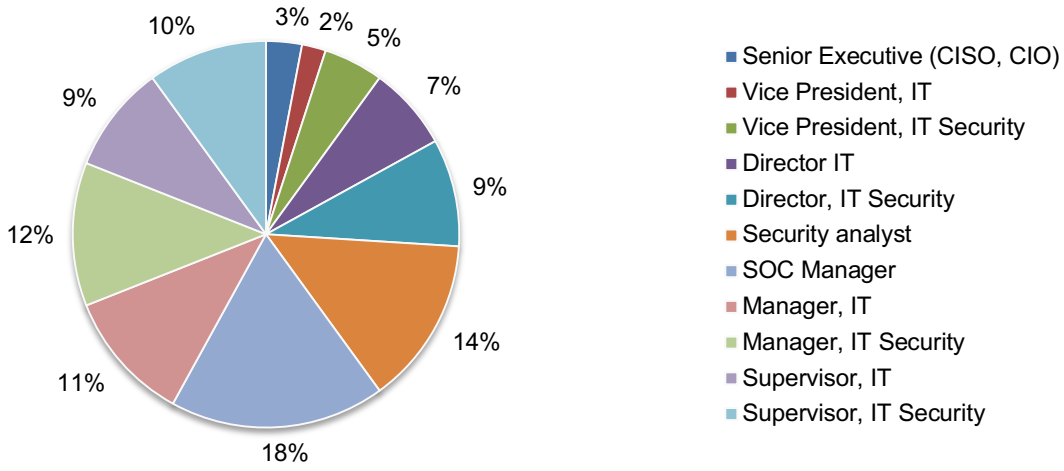
Part 3. Methods

A sampling frame of 16,841 IT and IT security practitioners that have a SOC and are knowledgeable about cybersecurity practices in their organizations were selected as participants in this survey. Table 1 shows 701 total returns. Screening and reliability checks required the removal of 64 surveys. Our final sample consisted of 637 surveys or a 3.8 percent response.

Table 1. Survey response	FY2019	Pct%
Total sampling frame	16,841	100.0%
Total returns	701	4.2%
Rejected surveys	64	0.4%
Final sample	637	3.8%

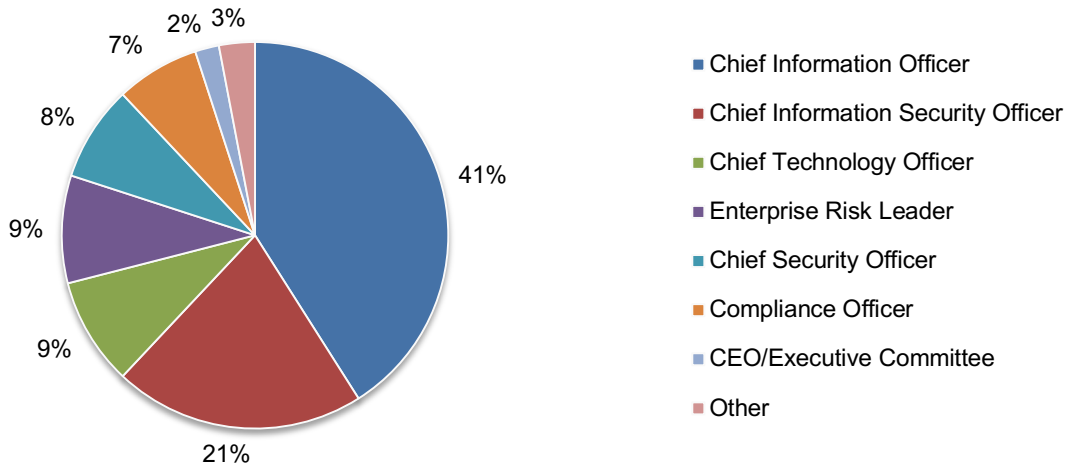
The following pie chart summarizes the position level of qualified respondents. At 18 percent, the largest segment contains those respondents who are SOC managers. Fourteen percent of respondents reported their position level security analyst.

Pie Chart 1. Position level of respondents



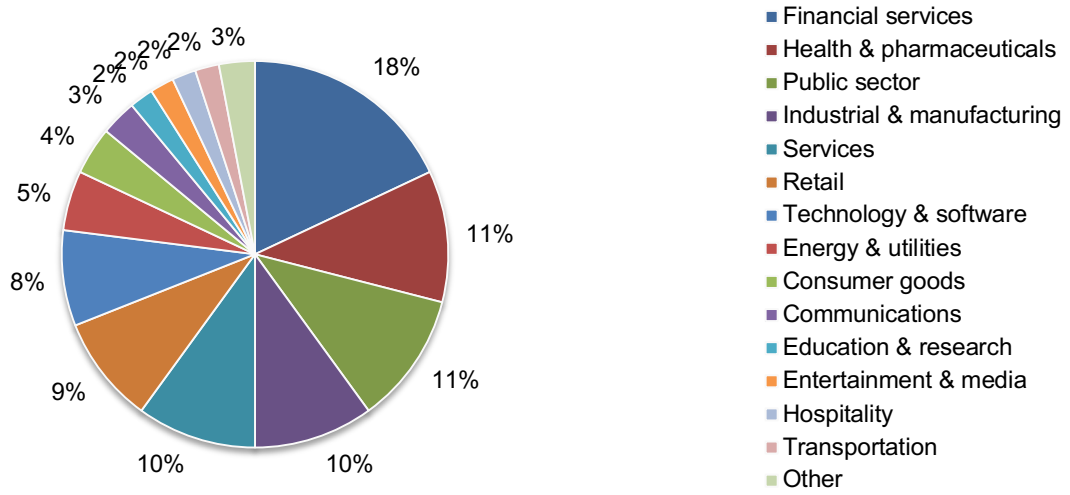
Pie Chart 2 reports the respondents' direct reporting channels. Forty-one percent of respondents report to the chief information officer, 21 percent of respondents report to the chief information security officer, 9 percent of respondents report to the chief technology officer and another 9 percent of respondents report to the enterprise risk leader.

Pie Chart 2. Primary Person you or your IT security leader reports to within the organization



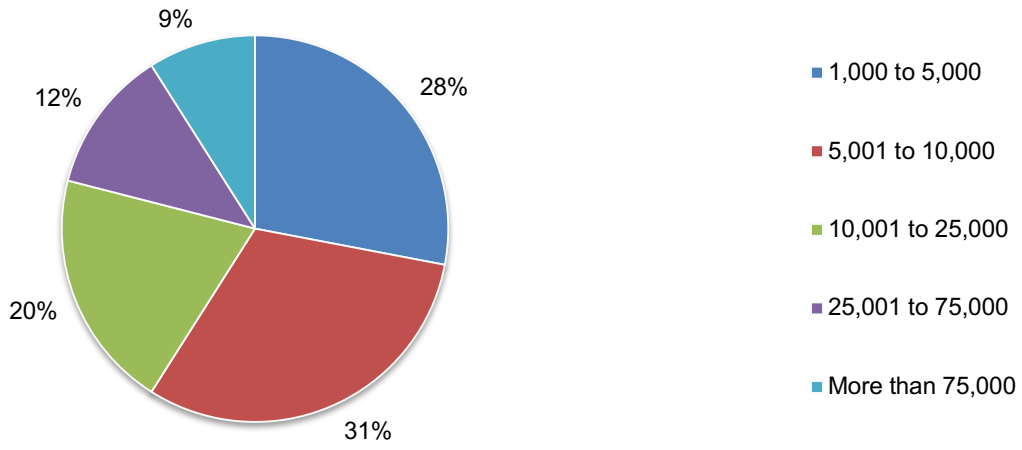
Pie Chart 3 reports the industry focus of respondents' organizations. The largest industry classification is financial services (18 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (11 percent of respondents), public sector (11 percent of respondents), industrial and manufacturing (10 percent of respondents) and services (10 percent of respondents).

Pie Chart 3. Industry focus of respondents' organizations



As shown in Pie Chart 4, more than half (59 percent) of respondents are from organizations with a worldwide headcount from 1,000 to 10,000 employees.

Pie Chart 4. Worldwide headcount of respondents' organizations



Part 4. Caveats

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

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

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals that have a SOC and are knowledgeable about cybersecurity practices in their organizations. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured October 10 to October 25, 2019.

Survey response	Freq	Pct%
Total sampling frame	16,841	100.0%
Total returns	701	4.2%
Rejected surveys	64	0.4%
Final sample	637	3.8%

Part 1. Screening

S1. Does your organization employ a SOC?	Pct%
Yes, it is on-premise	32%
Yes, it is outsourced (i.e. MSSP)	21%
Yes, it is a combination of on-premise and outsourced	27%
No (stop)	20%
Total	100%

S2. In your organization, which of the following are you responsible for or supervise? Please select all that apply.	Pct%
Information security	53%
Data privacy	1%
Governance, risk and compliance	26%
Incident response & management	37%
Network security architecture	17%
Security for virtualized or cloud networks	16%
Threat detection and remediation	49%
Vulnerability assessment and penetration testing	42%
Identity management	26%
Security operations management (SOM/SOC)	48%
Network or IT operations (NOC)	39%
None of the above (stop)	0%
Total	354%

Part 2. Background

Q1. What are the top security challenges your organization faces? Please select your top three choices.	Pct%
Negligent insiders	34%
System glitches (including process failure)	12%
Malicious or criminal insiders	15%
Web-based attacks	23%
Insecure web applications	27%
Insecure endpoints	32%
Third-party mistakes or flubs (including cloud providers)	29%
Third-party IT security risks	30%
DNS-based denial of service attacks	21%
Electronic agents such as viruses, worms, malware, botnets and others	34%
Nation-state, terrorist or criminal syndicate sponsored attacks	21%
Deliberate theft of key intellectual property	22%
Other (please specify)	0%
Total	300%

Q2. Following are core services typically deployed within the SOC environment. Please check all SOC services provided today.	Pct%
Management of security intelligence technologies	33%
Network security management (NSM)	25%
Endpoint detection and response (EDR)	38%
Monitored or managed firewalls or intrusion prevention systems (IPSs)	59%
Monitored or managed intrusion detection systems (IDSs)	55%
Monitored or managed multifunction firewalls, or unified threat management (UTM) technology	56%
Managed or monitored security gateways for messaging or Web traffic	34%
Security analysis and reporting of events collected from IT infrastructure logs	26%
Reporting associated with monitored/managed devices and incident response	34%
Managed vulnerability scanning of networks, servers, databases or applications	53%
Distributed denial of service (DDoS) protection	45%
Malware protection & defense	44%
Maintenance, tuning and updates on security sensors	43%
Monitoring of advanced threats	37%
Use of honeypot deception and other countermeasures	17%
Threat hunting	41%
Incident response and remediation	39%
Other (please specify)	3%
Total	682%

Q3. How important is your organization's SOC to its overall cybersecurity strategy?	Pct%
Essential	31%
Very important	42%
Important	20%
Not important	5%
Irrelevant	2%
Total	100%

Q4. What best defines the IT infrastructure monitored by your SOC?	Pct%
Cloud	31%
On-premise	34%
Mobile	9%
Combination of cloud and on-premise (hybrid)	26%
Total	100%

Q5. Who **leads** your organization's SOC team? Please select only one choice.	Pct%
Chief information officer	20%
Chief technology officer	4%
Chief information security officer	21%
Director of security operations	15%
Chief security officer	3%
Head, enterprise risk management	5%
Head, lines of business (LOB)	16%
No one function (shared ownership)	16%
Other (please specify)	0%
Total	100%

Part 3. How much do SOCs cost?

Q6. How many of your organization's IT security personnel and/or contractors are assigned to the SOC?	Pct%
None	8%
Less than 5	16%
5 to 10	36%
11 to 25	24%
More than 25	16%
Total	100%
Extrapolated value	12.10

Q7a. What is the average salary for a tier one analyst?	Pct%
Less than $50,000	2%
$50,001 to $75,000	14%
$ 75,001 to $100,000	45%
$100,001 to $150,000	30%
More than $150,000	9%
Total	100%
Extrapolated value	$102,315

Q7b. How will this average salary change in 2020?	Pct%
Significantly increase	15%
Increase	30%
Stay the same	37%
Decrease (please skip to Q7d)	10%
Significantly decrease (please skip to Q7d)	8%
Total	100%

Q7c. If the salary will significantly increase or increase, what is the average percentage increase?	Pct%
Less than 5 percent	4%
5 percent to 10 percent	15%
11 percent to 25 percent	32%
26 percent to 50 percent	31%
More than 50 percent	18%
Total	100%
Extrapolated value	29%

Q7d. If the salary will significantly decrease or decrease, what is the average percentage decrease?	Pct%
Less than 5 percent	0%
5 percent to 10 percent	6%
11 percent to 25 percent	48%
26 percent to 50 percent	43%
More than 50 percent	3%
Total	100%
Extrapolated value	27%

Q8. How many analysts will be hired in 2020?	Pct%
None	13%
1 to 2	15%
3 to 5	52%
6 to 10	12%
More than 10	8%
Total	100%
Extrapolated value	4.1

Q9. On average, how many analysts resign or are fired in one year?	Pct%
None	15%
1 to 2	37%
3 to 5	35%
6 to 10	13%
More than 10	0%
Total	100%
Extrapolated value	3.0

Q10. On average, how long does an analyst stay in the position?	Pct%
Less than 6 months	3%
6 months to 12 months	9%
13 months to 24 months	25%
25 months to 36 months	37%
More than 36 months	26%
Total	100%
Extrapolated value (months)	27.2

Q11. What is the average time spent **hiring** one analyst?	Pct%
Less than a month	2%
1 to 2 months	23%
3 to 4 months	43%
More than 4 months	32%
Total	100%
Extrapolated value (months)	3.5

Q12. What is the average time spent **training** one analyst?	Pct%
Less than a month	0%
1 to 2 months	21%
3 to 4 months	34%
More than 4 months	45%
Total	100%
Extrapolated value (months)	3.8

Part 4. SOC effectiveness

Q13. Does your organization partially or completely outsource security operations monitoring to a MSSP?	Pct%
Yes, partially outsource	23%
Yes, completely outsource	28%
No, we do not outsource (please skip to Q18)	49%
Total	100%

Q14. If yes, what is the annual cost of outsourcing to a MSSP?	Pct%
Less than $100,000	2%
$100,001 to $250,000	6%
$250,001 to $500,000	12%
$500,001 to $1,000,000	26%
$1,000,001 to $5,000,000	28%
$5,000,001 to $10,000,000	16%
$10,000,001 to $25,000,000	8%
$25,000,001 to $50,000,000	2%
More than $50,000,000	0%
Total	100%
Extrapolated value	$4,442,500

Q15. Using the following 10-point scale, please rate the effectiveness of your organization's MSSP on a scale of 1 = not effective to 10 = very effective	Pct%
1 or 2	8%
3 or 4	18%
5 or 6	32%
7 or 8	25%
9 or 10	17%
Total	100%
Extrapolated value	6.00

Q16. If not effective (responses 1 to 4), what actions does your organization plan to take?	Pct%
Our organization is considering working with another vendor	23%
Our organization will continue working with our MSSP because it is too difficult to transition to another vendor	16%
Our organization will continue working with our MSSP because it is locked into a contract	21%
Our organization plans to bring the SOC in-house	40%
Other (Please specify)	0%
Total	100%

Q17. Using the following 10-point scale, please rate the "pain" your organization's SOC security personnel experience in meeting their daily job requirements.	Pct%
1 or 2	6%
3 or 4	7%
5 or 6	15%
7 or 8	25%
9 or 10	47%
Total	100%
Extrapolated value	7.50

Q18. What makes working in the SOC painful (7+ responses)? Please select all that apply.	Pct%
Information overload	65%
Lack of resources	52%
Increasing workload causes burnout	75%
Being on call 24/7/365	69%
Inability to capture actionable intelligence	53%
Too many alerts to chase	65%
Inability to prioritize threats	58%
Lack of visibility into the network and IT infrastructure	68%
Inability to effectively collaborate with IT teams to manage threats and risks	44%
Inability to recruit and retain expert personnel	64%
Complexity and chaos in the SOC	54%
Losing to adversaries	49%
Other (please specify)	1%
Total	717%

Q19. Using the following 10-point scale, please rate the complexity of managing your organization's SOC from 1 = low complexity to 10 = high complexity.	Pct%
1 or 2	3%
3 or 4	6%
5 or 6	17%
7 or 8	24%
9 or 10	50%
Total	100%
Extrapolated value	7.74

Q20. Using the following 10-point scale, please rate the effectiveness of your organization's SOC in detecting attacks from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	7%
3 or 4	13%
5 or 6	29%
7 or 8	30%
9 or 10	21%
Total	100%
Extrapolated value	6.40

Q21. Using the following 10-point scale, please rate how much those responsible for hiring and training SOC analysts believe it has a negative impact on their ability to complete their other responsibilities from 1 = no impact to 10 = high impact	Pct%
1 or 2	5%
3 or 4	10%
5 or 6	20%
7 or 8	33%
9 or 10	32%
Total	100%
Extrapolated value	7.04

Q22. Using the following 10-point scale, please rate the ability to hire the right talent for your organization's SOC on a scale from 1= low ability to 10 = high ability.	Pct%
1 or 2	14%
3 or 4	10%
5 or 6	25%
7 or 8	33%
9 or 10	18%
Total	100%
Extrapolated value	6.12

Part 5. Attributions

Please rate the following statements using the agreement scale below each item.	
Q23. The ROI of our organization's SOC is getting worse, not better.	Pct%
Strongly agree	23%
Agree	21%
Unsure	11%
Disagree	27%
Strongly disagree	18%
Total	100%

Q24. Our SOC analysts burn out quickly because of the high-pressure environment.	Pct%
Strongly agree	38%
Agree	32%
Unsure	10%
Disagree	11%
Strongly disagree	9%
Total	100%

Part 6. The importance of SOC activities

Using the following 10-point scale, please rate the importance of the following 10 SOC activities to being able to stop intruders from 1 = low importance to 10 = high importance.

Q25. Threat hunting	Pct%
1 or 2	3%
3 or 4	8%
5 or 6	18%
7 or 8	36%
9 or 10	35%
Total	100%
Extrapolated value	7.34

Q26. Cyber forensics	Pct%
1 or 2	5%
3 or 4	9%
5 or 6	17%
7 or 8	35%
9 or 10	34%
Total	100%
Extrapolated value	7.18

Q27. Threat intelligence reporting	Pct%
1 or 2	0%
3 or 4	8%
5 or 6	9%
7 or 8	33%
9 or 10	50%
Total	100%
Extrapolated value	8.00

Q28. Intrusion detection	Pct%
1 or 2	2%
3 or 4	5%
5 or 6	16%
7 or 8	40%
9 or 10	37%
Total	100%
Extrapolated value	7.60

Q29. Incident response	Pct%
1 or 2	5%
3 or 4	8%
5 or 6	12%
7 or 8	39%
9 or 10	36%
Total	100%
Extrapolated value	7.36

Q30. Training SOC analysts	Pct%
1 or 2	3%
3 or 4	11%
5 or 6	19%
7 or 8	36%
9 or 10	31%
Total	100%
Extrapolated value	7.12

Q31. Collaboration with other IT functions	Pct%
1 or 2	2%
3 or 4	13%
5 or 6	10%
7 or 8	42%
9 or 10	33%
Total	100%
Extrapolated value	7.32

Q32. Minimization of false positives	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	13%
7 or 8	39%
9 or 10	45%
Total	100%
Extrapolated value	8.02

Q33. Monitoring and analyzing alerts	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	20%
7 or 8	35%
9 or 10	42%
Total	100%
Extrapolated value	7.82

Q34. The use of technologies such as automation and machine	Pct%
1 or 2	5%
3 or 4	9%
5 or 6	14%
7 or 8	30%
9 or 10	44%
Total	102%
Extrapolated value	7.59

Q35. Agile DevOps	Pct%
1 or 2	8%
3 or 4	8%
5 or 6	11%
7 or 8	33%
9 or 10	40%
Total	100%
Extrapolated value	7.28

Part 7. Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive (CISO, CIO)	3%
Vice President, IT	2%
Vice President, IT Security	5%
Director IT	7%
Director, IT Security	9%
Security analyst	14%
SOC Manager	18%
Manager, IT	11%
Manager, IT Security	12%
Supervisor, IT	9%
Supervisor, IT Security	10%
Other (please specify)	0%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/Executive Committee	2%
Chief Financial Officer	0%
General Counsel	1%
Chief Information Officer	41%
Chief Technology Officer	9%
Compliance Officer	7%
Human Resources VP	0%
Chief Security Officer	8%
Chief Information Security Officer	21%
Enterprise Risk Leader	9%
Other (please specify)	2%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer goods	4%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceuticals	11%
Hospitality	2%
Industrial & manufacturing	10%
Public sector	11%
Retail	9%
Services	10%
Technology & software	8%
Transportation	2%
Other (please specify)	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
1,000 to 5,000	28%
5,001 to 10,000	31%
10,001 to 25,000	20%
25,001 to 75,000	12%
More than 75,000	9%
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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.