The Importance of Cyber Threat Intelligence to a Strong Security Posture

Sponsored by Webroot

Independently conducted by Ponemon Institute LLC

Publication Date: March 2015

The Importance of Cyber Threat Intelligence to a Strong Security Posture

Ponemon Institute, March 2015

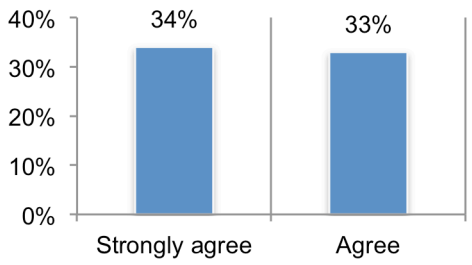
Part 1. Introduction

Does access to timely, accurate and actionable cyber threat intelligence[1] make a difference in blocking or preventing external attacks? Are companies using cyber threat intelligence effectively to make informed decisions about how to respond to a menace or hazard?

Ponemon Institute is pleased to present *The Importance of Cyber Threat Intelligence to a Strong Security Posture,* sponsored by Webroot. The purpose of the study is to understand how companies are using, gathering and analyzing threat intelligence as part of their IT security strategy. We surveyed 693 IT and IT security practitioners in the United States who are familiar with their company's security strategy or approach to cyber threat intelligence. Sixty-one percent of respondents are in the *Fortune 1,000, Global 2,000* and the *Forbes List of the Largest Private Companies.*

The organizations represented in this research have one or more staff members dedicated to threat intelligence. As shown in Figure 1, 67 percent of respondents believe the use of threat intelligence provides benefits that outweigh the cost. However, as revealed in this research, improvements are needed to make threat intelligence more timely, accurate and actionable in order to strengthen an organization's security posture.

Figure 1. The use of threat intelligence provides benefits that outweigh cost



Following are reasons why respondents believe cyber threat intelligence supports a strong security posture:

- On average, organizations report since using threat intelligence 35 cyber attacks that eluded traditional defenses were uncovered.
- Real-time reputation intelligence is an effective way to detect and respond to malicious IPs the moment they appear within their infrastructure, according to 60 percent of respondents.
- Monitoring the good and bad of IPs, URLs, files and mobile apps that are related to an unknown object is an effective way to predict if they pose a security risk, according to 53 percent of respondents.
- Continual monitoring and tracking of changes in IPs, URLs, files and mobile apps in real time is essential to decreasing security incidents, according to 54 percent of respondents.
- Those companies using threat indicators say the following information is most useful: software vulnerability patch updates (67 percent of respondents), indicators of malicious IP addresses (57 percent of respondents) and indicators of malicious malware (55 percent of respondents).

[1] In the context of this research, threat intelligence is evidence-based knowledge that includes context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets.

Part 2. Key findings

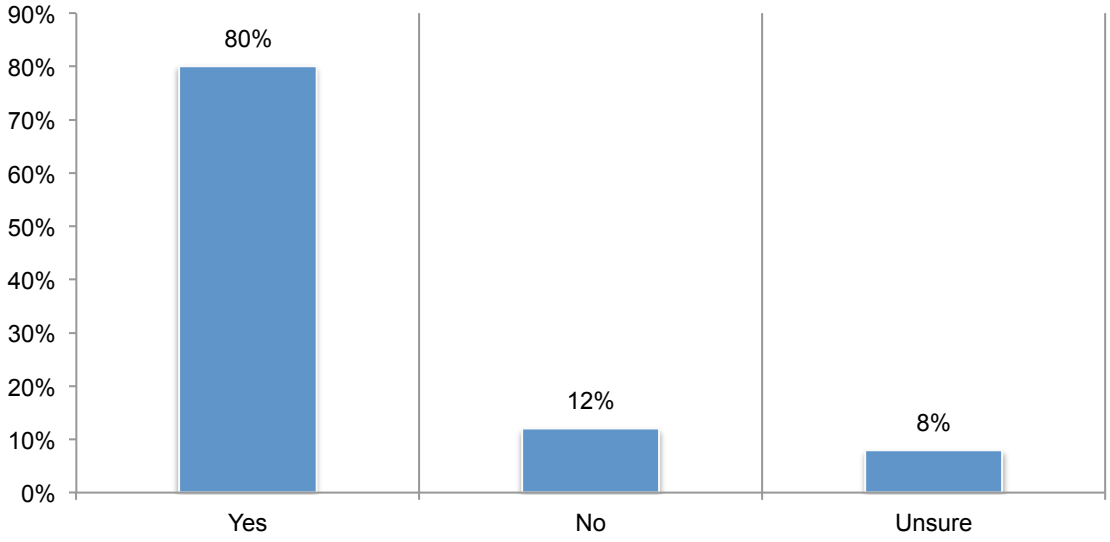
In this section, we present an analysis of the key findings of this research. The complete audited findings are presented in the appendix of this report. We have organized the findings according to the following topics:

- The importance of threat intelligence to building a strong cybersecurity posture
- The current state of threat intelligence in organizations
- What companies are spending on threat intelligence
- How threat intelligence can be improved
- Special analysis: threat intelligence differences between large and small companies

The importance of threat intelligence to building a strong cybersecurity posture

Threat intelligence is critical to an organization's security posture. Forty percent of companies in this research had a material security breach[2] in the past 24 months. During the past 24 months, 80 percent of these respondents believe if they had threat intelligence at the time of the breach they could have prevented or minimized the consequences of the attack, as shown in Figure 2.

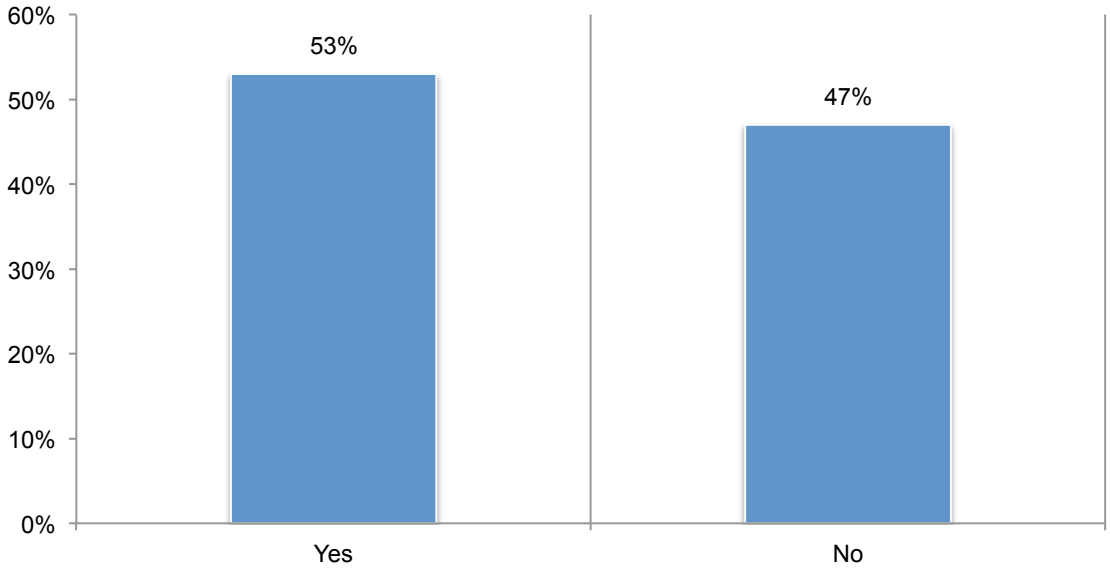
Figure 2. Would threat intelligence have helped prevent or minimize the consequences of an attack?



[2] A material security breach is defined as an attack that compromises the company's networks or enterprise systems. The attack or compromise can be internal (i.e., malicious insider), external (i.e., hacker) or both.

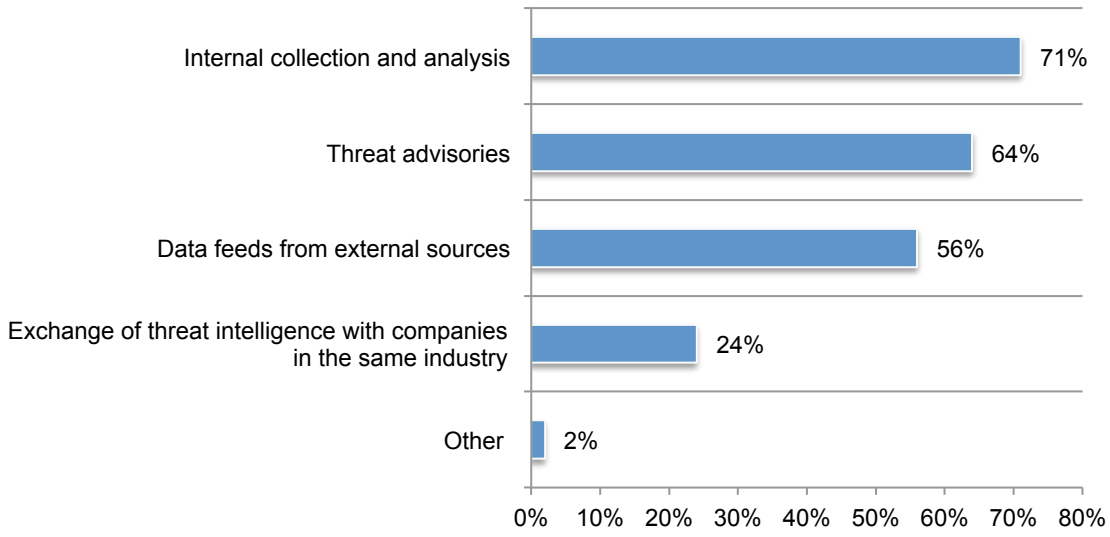
The majority of respondents believe threat intelligence is essential to a strong security posture. As shown in Figure 3, 53 percent say threat intelligence is critical. However, many respondents (47 percent) do not agree. A possible explanation is that the quality of threat intelligence has not evolved to the point where it would be a critical component of an IT security strategy.

Figure 3. Is cyber threat intelligence essential to a strong security posture?



According to Figure 4, threat intelligence is mostly received by internal collection and analysis (71 percent of respondents) or threat advisories (64 percent of respondents). Only 24 percent of respondents say they exchange threat intelligence with companies in the same industry. Fifty-six percent of respondents say they receive data feeds from external sources.

Figure 4. How is threat intelligence received by your organization?
More than one response permitted

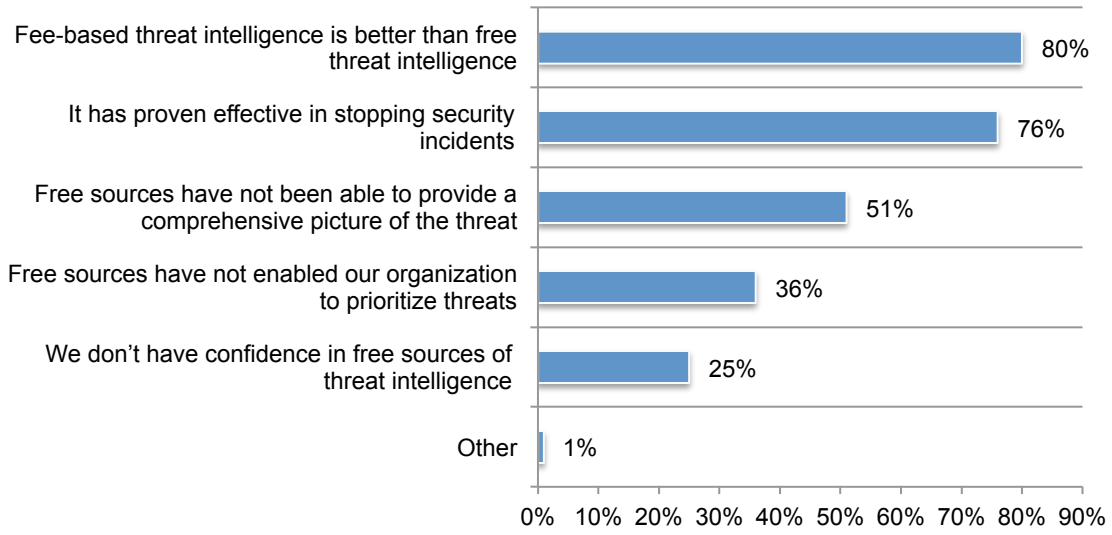


Do companies choose "Free" or "Fee" threat intelligence?

Why companies pay for threat intelligence. Forty-nine percent use "fee-based" sources of intelligence. As shown in Figure 5, the most common reason is the belief that it is better than "free" sources of threat intelligence (80 percent of respondents) followed by 76 percent of respondents who say it has proven effective in stopping security incidents. Respondents also cite free sources as not being able to show a comprehensive picture of the threat and not making it possible to prioritize threats.

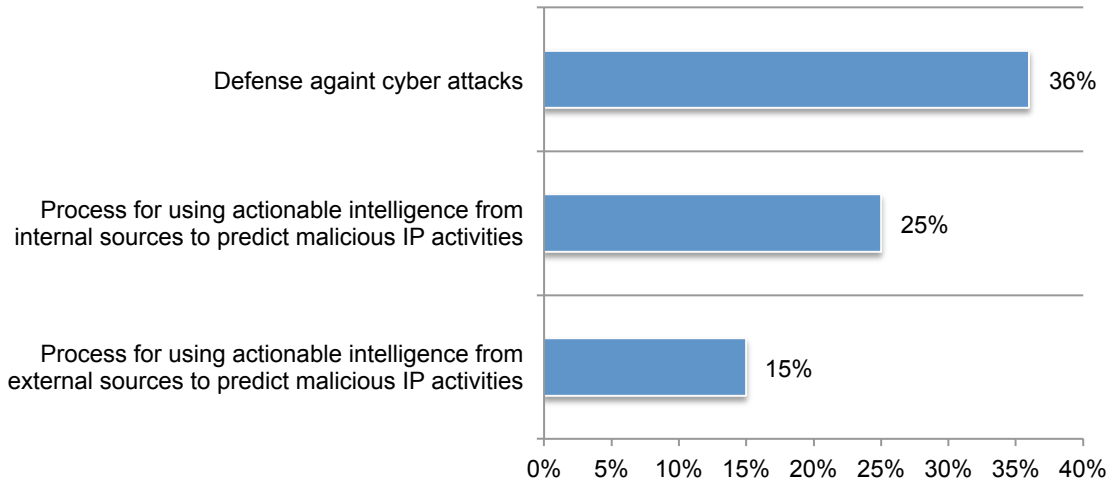
The department most responsible for deciding what threat intelligence sources, such as free or fee-based, are used is the chief information security officer (24 percent of respondents) followed by line of business senior management (22 percent of respondents) and 18 percent say it is a shared responsibility.

Figure 5. Why do companies pay for threat intelligence?
More than one response permitted



Current cyber defense practices are not considered effective. Figure 6 reveals that only 15 percent of respondents say their process for using actionable intelligence from external sources, such as vendor-supplied threat feeds to predict malicious IP effectives, is highly effective. Twenty-five percent of respondents say they are highly effective in using actionable intelligence from internal sources. Thirty-six percent rate their company's defense against cyber attacks as strong.

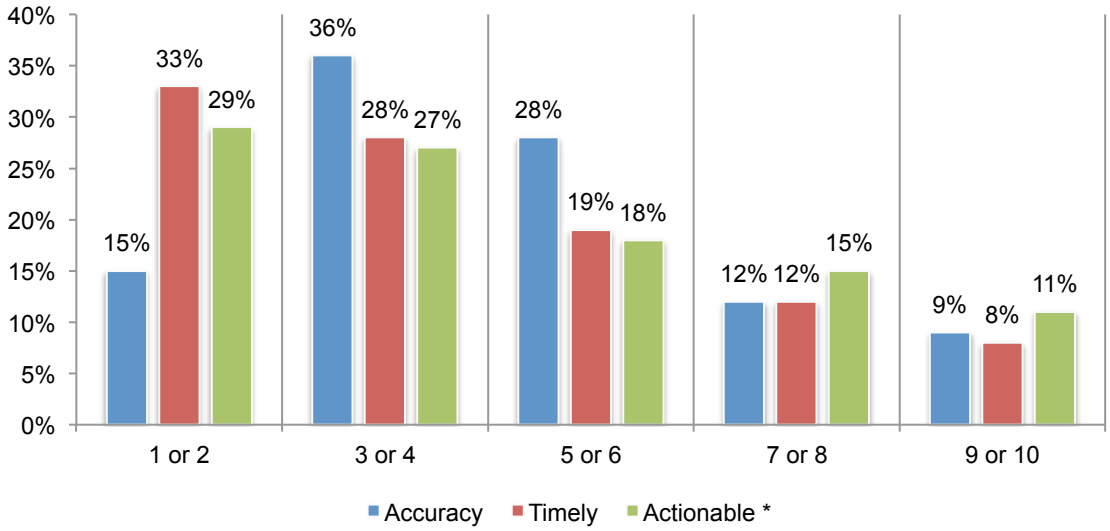
Figure 6. How effective is your cyber defense?
On a scale of 1 = low effectiveness to 10 = highly effective, the percentage of respondents who rated effectiveness 7 or greater



The current state of threat intelligence in organizations

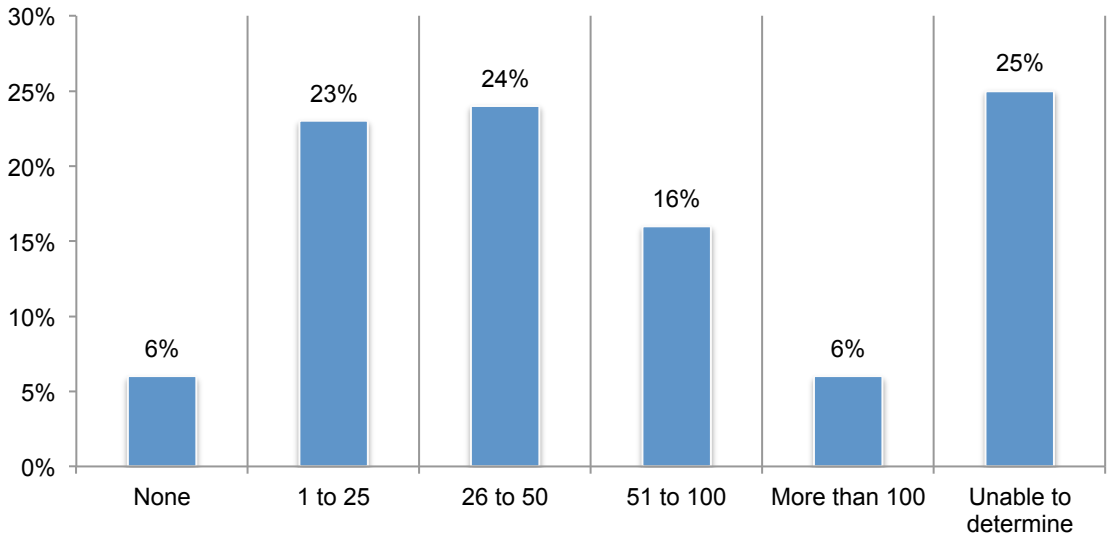
Many organizations are increasing the amount of intelligence data they consume but it is not considered reliable. As shown in Figure 7, 45 percent of respondents say they are increasing the amount of intelligence data they receive and 35 percent say it has stayed the same over the past 12 months. However, only 9 percent say the accuracy of the intelligence is reliable, 8 percent say it is timely and 11 percent say it is actionable.

Figure 7. How accurate, timely and actionable is your company's threat intelligence?
Scale: 1 = unreliable to 10 = very reliable; * Scale: 1 = not actionable to 10 = very actionable



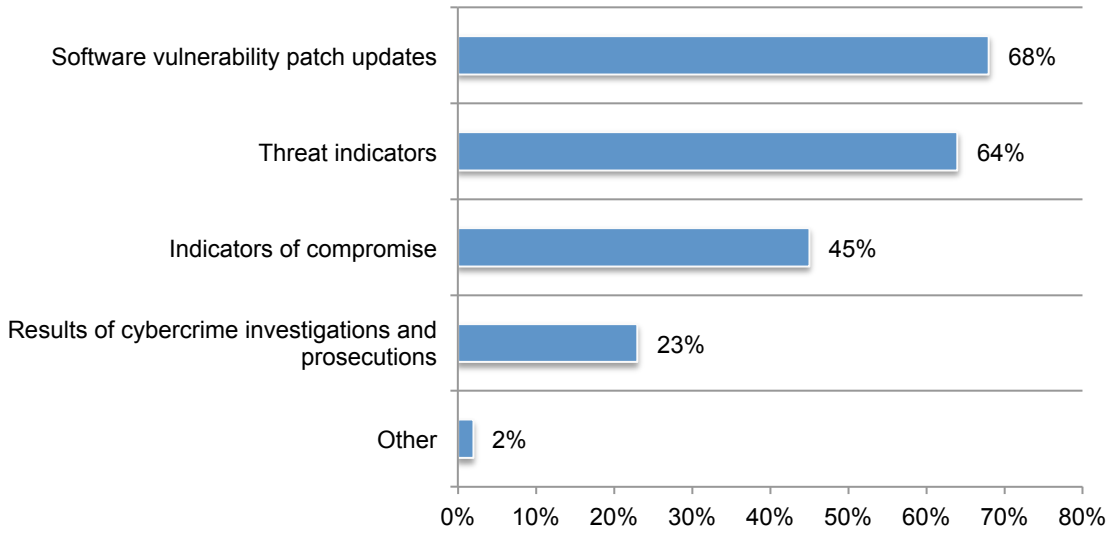
Companies in this study are increasing the amount of intelligence data they receive—even if it could be better—because it helps prevent or mitigate the consequences of an attack. As shown in Figure 8, on average, since adopting threat intelligence, organizations have been able to determine 35 cyber attacks that eluded traditional defenses because of threat intelligence from internal and external sources.

Figure 8. How many cyber attacks that eluded traditional defenses have you discovered because of threat intelligence?
Extrapolated average = 35



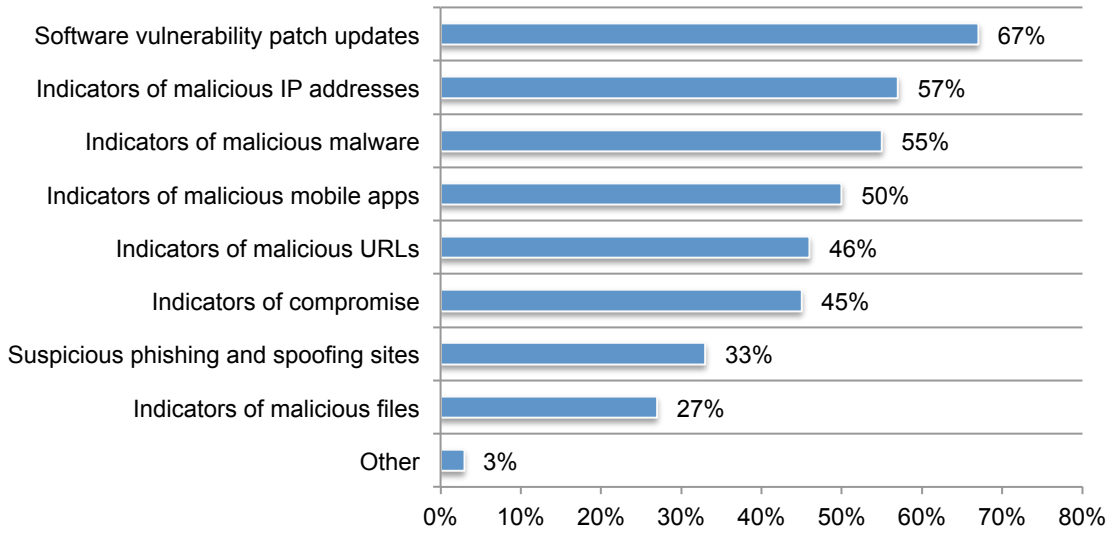
What types of threat intelligence are most often used? According to Figure 9, the threat intelligence most often used is software vulnerability patch updates (68 percent of respondents) or threat indicators (64 percent of respondents). Fewer organizations rely upon indicators of compromise (45 percent of respondents) or results of cybercrime investigations and prosecutions (23 percent of respondents).

Figure 9. What threat intelligence does your company use?
More than one response permitted



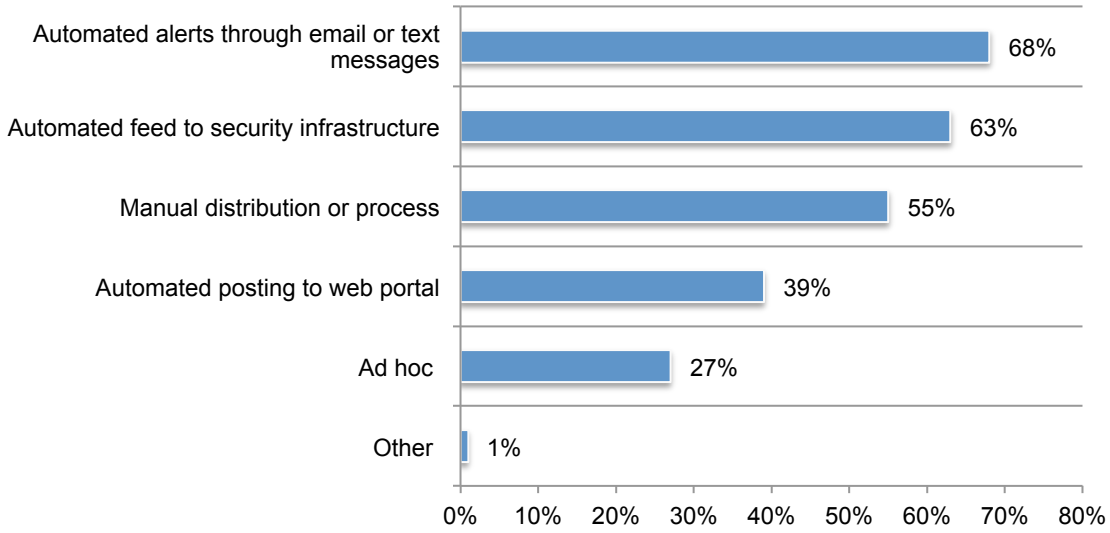
According to Figure 10, those organizations using threat indicators (64 percent of respondents) say the following information is most useful: software vulnerability patch updates (67 percent of respondents), indicators of malicious IP addresses (57 percent of respondents), indicators of malicious malware (55 percent of respondents).

Figure 10. If using threat indicators, what information is most valuable?
More than one response permitted



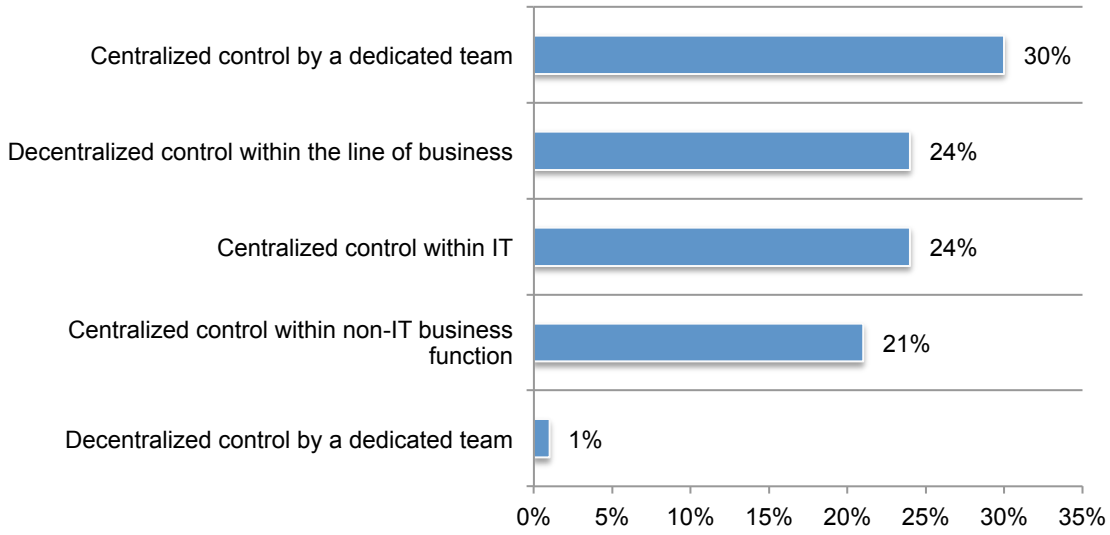
How are organizations managing threat intelligence? Threat intelligence is disseminated mostly by automated alerts through email or text messages (68 percent of respondents) and automated feed to security infrastructure (63 percent of respondents), as shown in Figure 11.

Figure 11. How do organizations disseminate threat intelligence throughout the organization? More than one response permitted



According to Figure 12, centralized control by a dedicated team, according to 30 percent of respondents is how they exchange threat intelligence within their organization. This is followed by centralized control within IT or decentralized control within the line of business (both 24 percent of respondents.

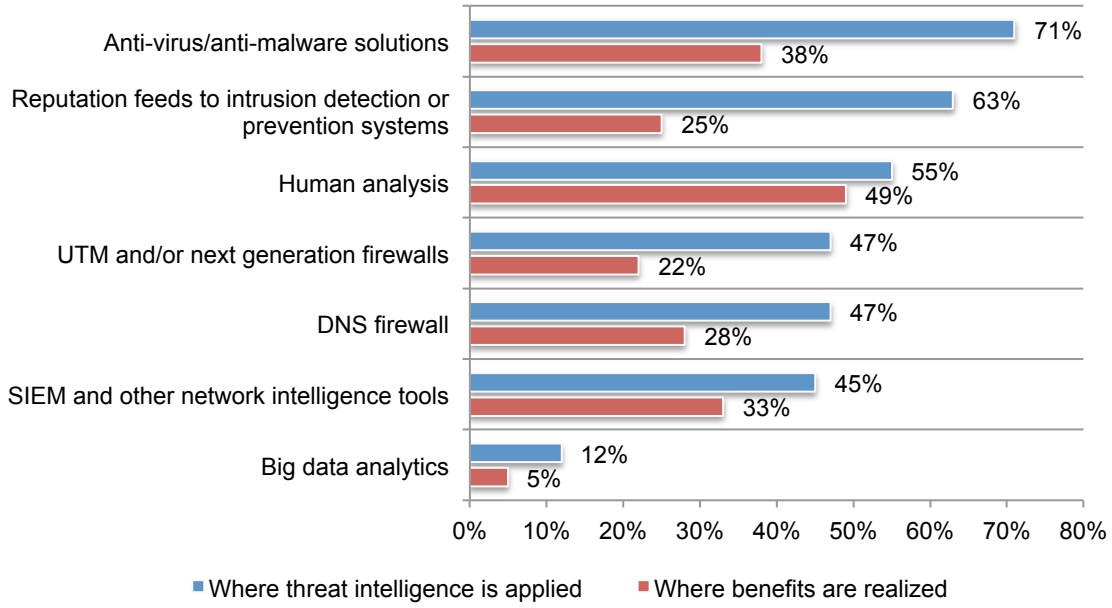
Figure 12. How threat intelligence is exchanged within the organization



Where organizations are applying threat intelligence is not necessarily where they realize the most benefit. Figure 13 reveals that anti-virus/anti-malware solutions (71 percent of respondents), reputation feeds to intrusion detection or prevention systems (63 percent of respondents) and human analysis are where organizations are applying threat intelligence.

Specifically, only 25 percent of respondents say they are realizing the most benefit from applying threat intelligence to reputation feeds to intrusion detection or prevention systems. Where organizations are receiving the most benefit from threat intelligence are: human analysis (49 percent of respondents) and anti-virus/anti-malware (38 percent of respondents).

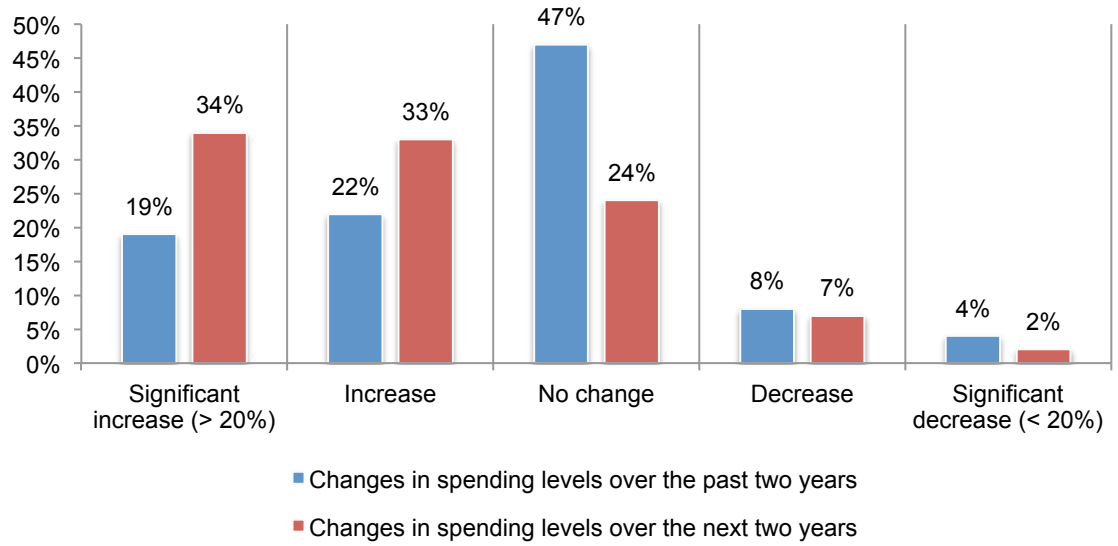
Figure 13. Where threat intelligence is applied and where the most benefits are realized
More than one response permitted



What companies spend on threat intelligence

Spending on threat intelligence is expected to increase over the next two years. In the past two years, 19 percent say their organizations' budget for threat intelligence increased significantly, according to Figure 14. In the next two years, 34 percent of respondents say their organizations will increase their threat intelligence budget significantly.

Figure 14. What companies are spending and will spend on threat intelligence



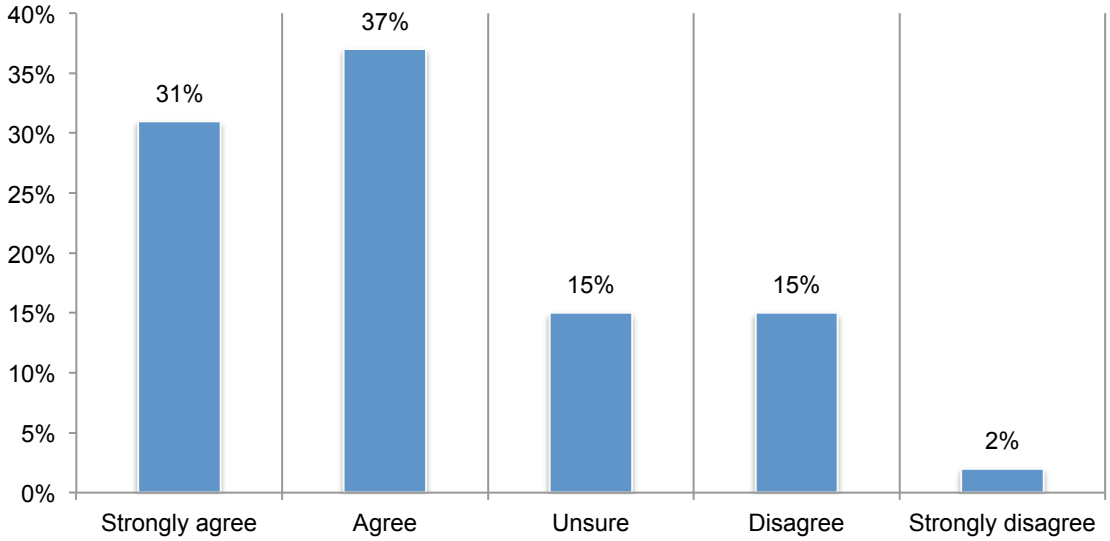
On average, organizations are spending $112 million on all IT operations, including licensing and maintenance fees, labor costs, investments in enabling technologies and overhead. On average, 7.4 percent is allocated to IT security and 9.3 percent of the IT security budget is allocated to threat intelligence operations (both internal and external combined).

Table 1. Threat intelligence budget and spending	Extrapolated value
Average budget for all IT operations	$112,340,000
Budget allocated to IT security	$8,262,533
Current year's IT security budget for both internal and external threat intelligence	$769,159

How threat intelligence can be improved

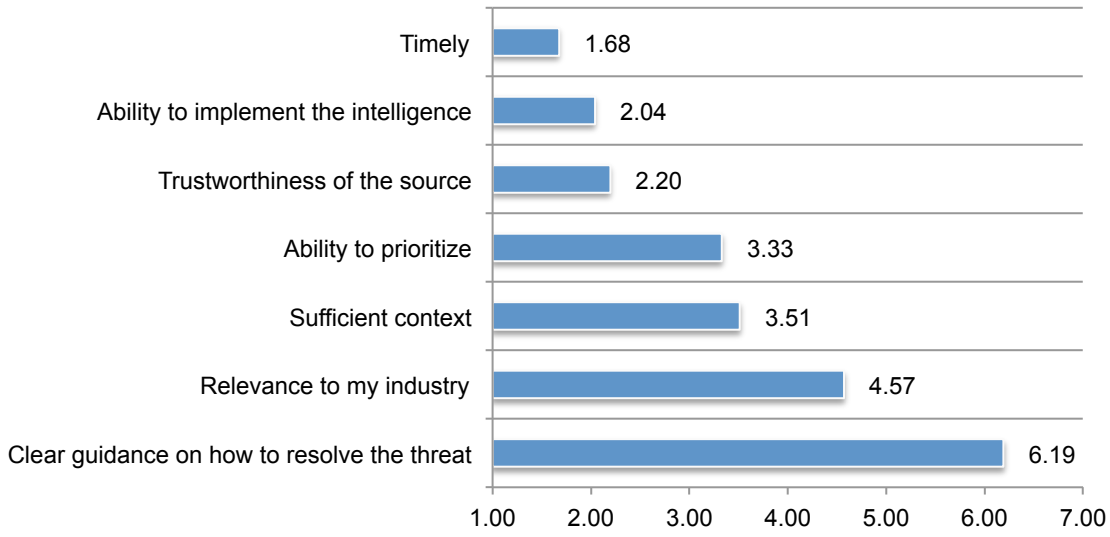
The use of cyber threat intelligence is important but issues such as too many alerts and false positives need to be addressed. As shown in Figure 15, respondents complain they receive too many alerts and false positives to make it possible to understand and respond to new threats.

Figure 15. Too many alerts and false positives is a problem



Threat intelligence needs to be timely and actionable. Fifty-six percent of respondents say intelligence becomes stale within seconds (21 percent of respondents) or within minutes (35 percent of respondents). The most important features, shown in Figure 16, timeliness, ability to implement intelligence and trustworthiness of the source are the most important features in a threat intelligence solution.

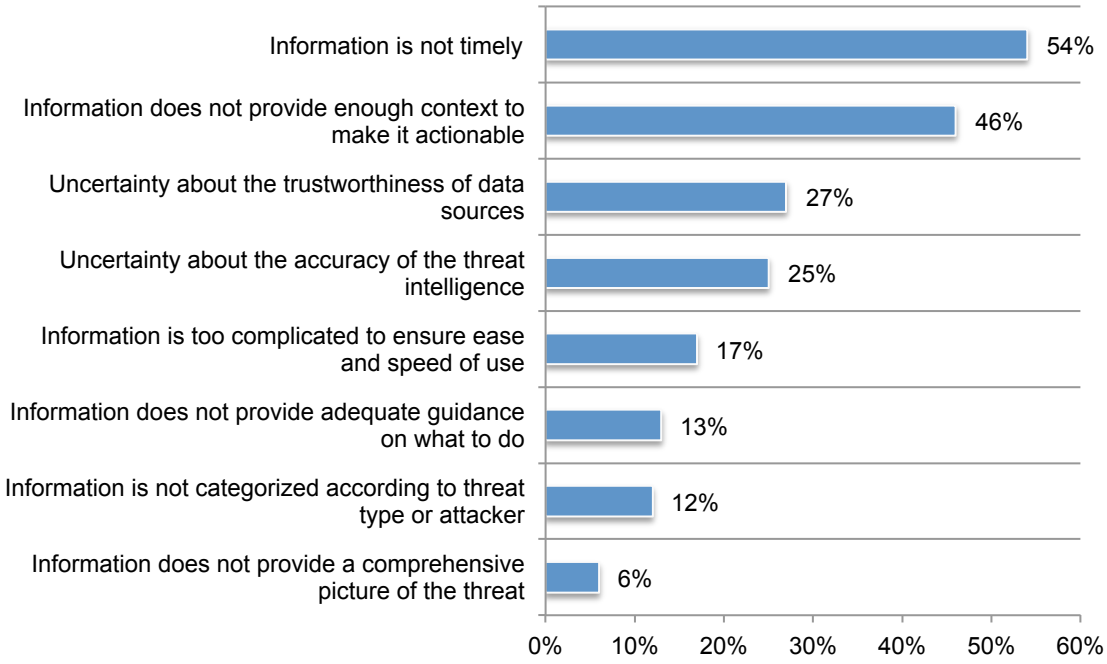
Figure 16. What features make threat intelligence actionable?
1 = most important to 7 = least important



Satisfaction with current threat intelligence is low. To ensure threat intelligence is actionable, it should be received as soon as possible. However, the research reveals that only 7 percent of respondents say they have access to it in real time and 11 percent say it is hourly. Twenty-nine percent say they receive it on demand.

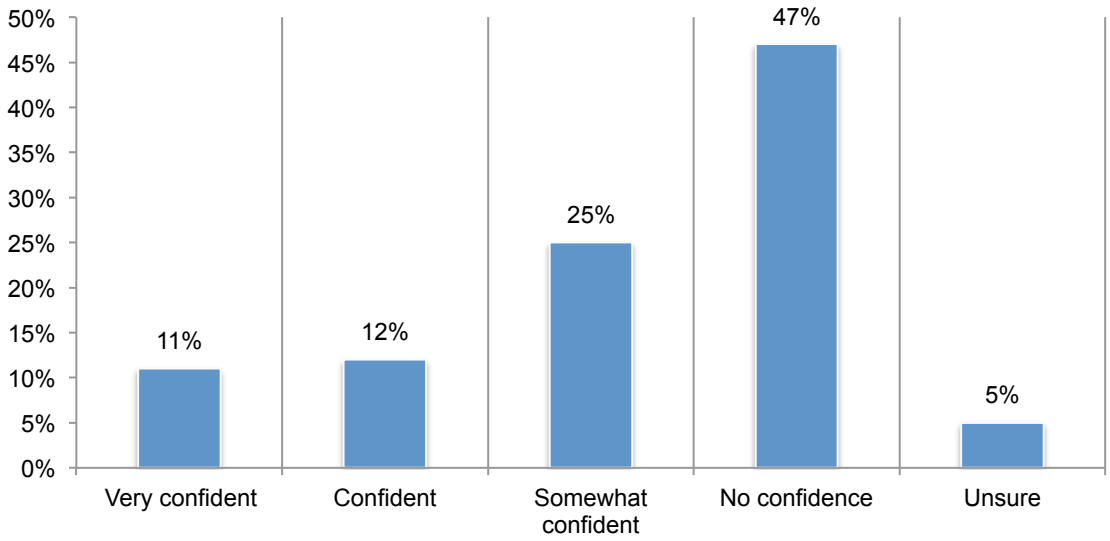
As shown in Figure 17, the main reasons they are not satisfied: information is not timely (54 percent) and does not provide enough context to make it actionable (46 percent).

Figure 17. Why are organizations not satisfied with the threat intelligence they receive?
More than one response permitted



Increase confidence in the sending threat intelligence to the cloud. There is a lack of confidence in sending threat intelligence data to the cloud for analysis. Figure 18 reveals currently, only 23 percent of respondents (11 percent + 12 percent) have confidence in the security of sending their organization's threat intelligence data to the cloud for analysis. Forty-seven percent have no confidence and 5 percent are unsure.

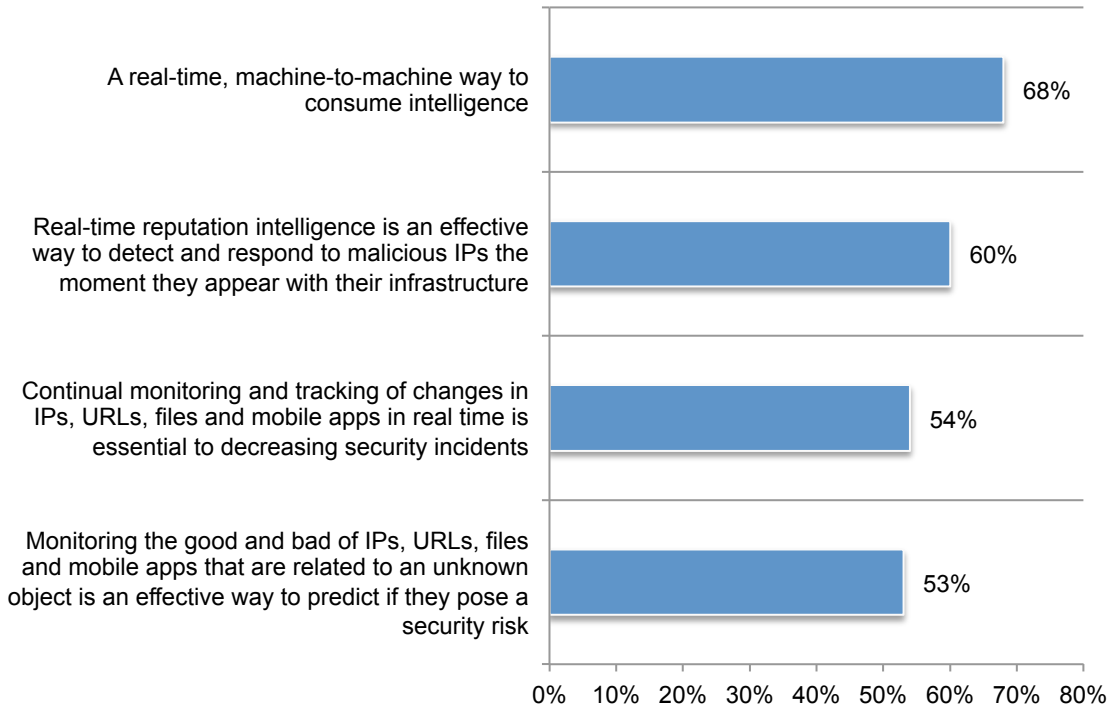
Figure 18. How confident are you that threat intelligence data sent to the cloud for analysis is secure?



How cyber intelligence creates a stronger security posture. Sixty-seven percent of respondents strongly agree or agree that the use of threat intelligence provides benefits that outweigh the cost. Figure 19 lists the attributes of an effective cyber intelligence strategy.

Real-time reputation intelligence is an effective way to detect and respond to malicious IPs the moment they appear with their infrastructure, (60 percent of respondents). Continual monitoring and tracking of changes in IPs, URLs, files and mobile apps in real time is essential to decreasing security incidents according to 54 percent of respondents. Monitoring the good and bad of IPs, URLs, files and mobile apps that are related to an unknown object is an effective way to predict if they pose a security risk, according to 53 percent of respondents.

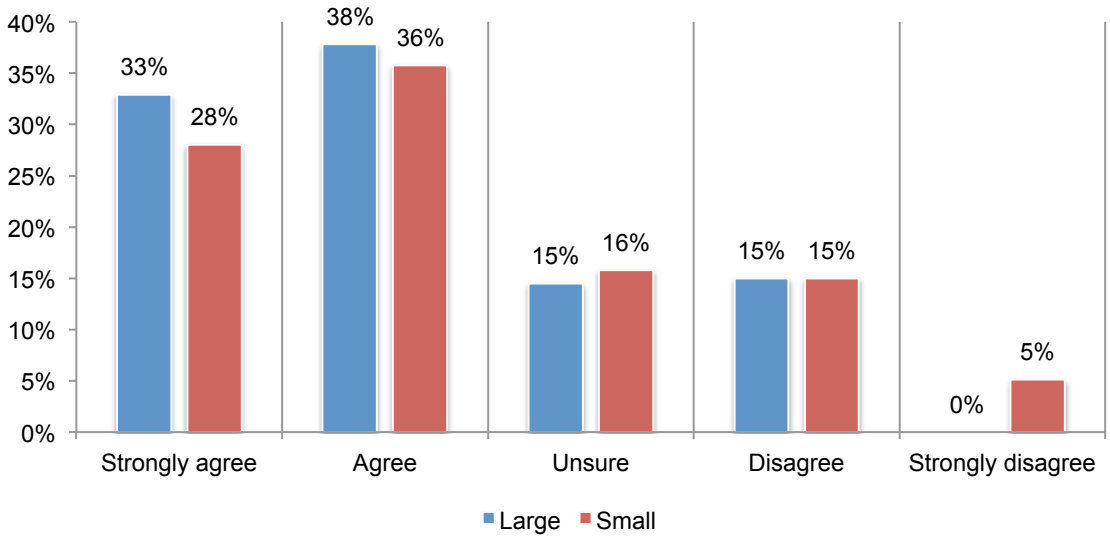
Figure 19. How to use cyber threat intelligence effectively
Strongly agree and agree response combined



Special analysis: threat intelligence differences between large and small companies

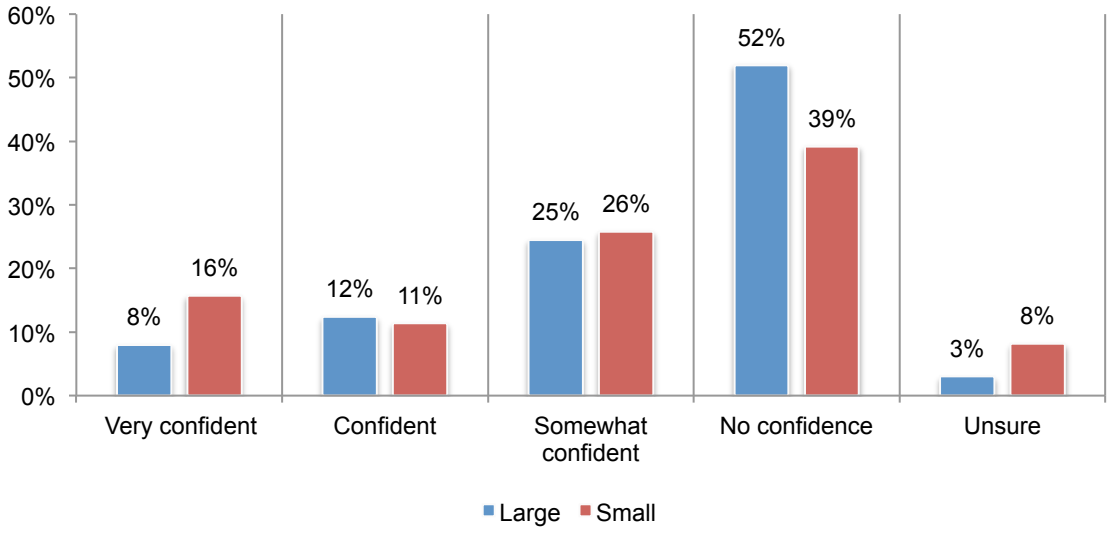
Does the size of a company influence its approach to cyber threat intelligence? In this study, 60 percent of respondents are in the *Fortune 1,000*, *Global 2,000* and the *Forbes* list of the largest private companies. Forty percent of respondents work in companies with approximately 500 or fewer employees. In general, the two groups are similar. However, the following findings indicate some interesting differences between these two groups. Larger companies are more likely to say they receive too many alerts and false positives. Seventy-one percent of larger companies vs. 64 percent of smaller companies experience too many alerts and false positives, as shown in Figure 20.

Figure 20. Our organization receives too many alerts and false positives



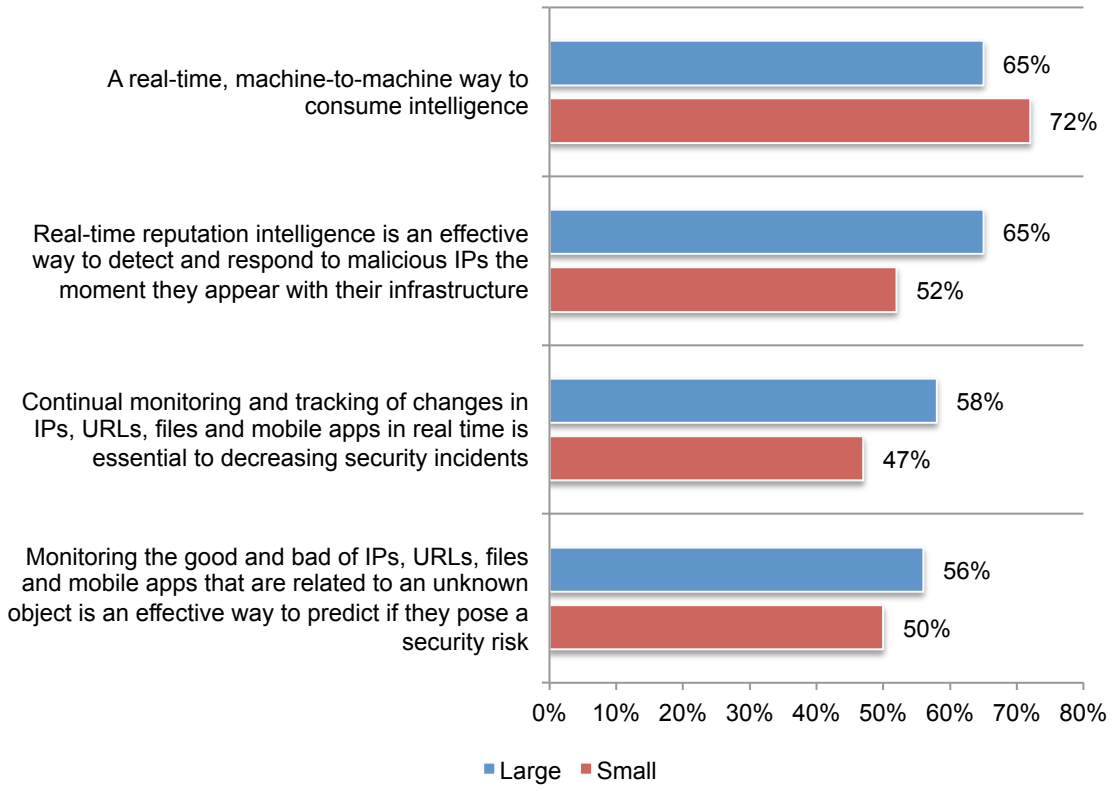
Large companies have less confidence in the security of sending threat intelligence to the cloud for analysis. As shown in Figure 21, 52 percent of respondents in larger companies have no confidence as opposed to 39 percent in smaller companies.

Figure 21. Confidence in the security of sending threat intelligence data to the cloud for analysis



As shown in Figure 22, there are differences in perceptions about what makes threat intelligence most effective. A real-time, machine-to-machine way to consume intelligence is considered more important for respondents in smaller companies (72 percent) vs. larger companies (65 percent). In contrast, larger companies see the other features listed in the figure as more effective.

Figure 22. Perceptions about how threat intelligence can be more effective
Strongly agree and agree



Part 3. Conclusion

The research findings reveal the gap in the perceptions and use of cyber threat intelligence. Increasingly, companies see the potential benefits and importance of having such information. In fact, most organizations have steadily increased their use of cyber threat intelligence. However, participants in this research are critical of the reliability of this intelligence as well as its ability to be actionable.

In addition to investing in the right technologies and solutions, organizations need to recognize the importance of having the in-house expertise to effectively use, gather and analyze the threat intelligence they are receiving. As revealed in the research, threat intelligence is not often applied to big data analytics, SIEM and other network intelligence tools that could improve the accuracy and reliability of threat intelligence. One possible deterrent to greater adoption is the lack of a knowledgeable and experienced staff.

In order to achieve a stronger security posture, organizations should consider adopting the following practices: monitoring the good and bad of IPs, URLs, files and mobile apps that are related to an unknown object in order to predict if they pose a security risk and continually monitor and track any changes in real time. Combining these approaches with experienced staff and the appropriate technologies will increase an organization's ability to minimize or prevent a serious security incident.

Part 4. Methods

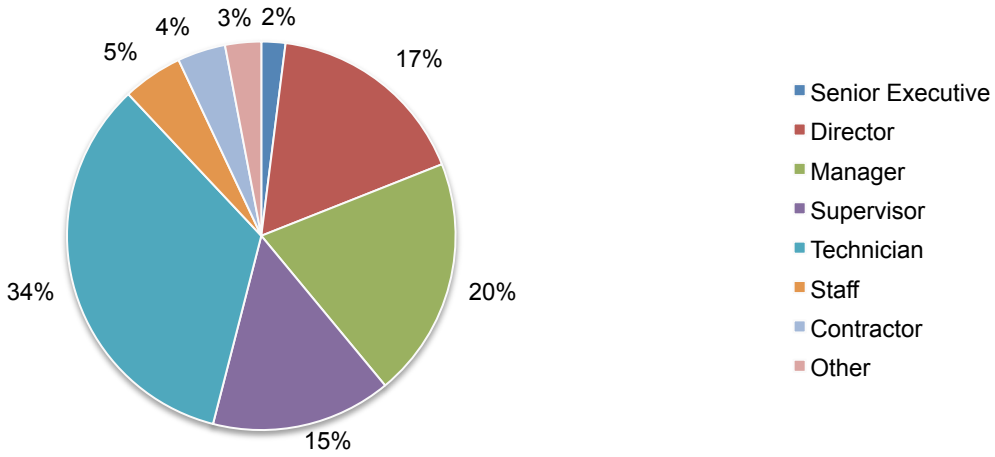
The sampling frame is composed of 19,811 IT and IT security practitioners located in the United States and who are familiar with their company's security strategy or approach to cyber threat intelligence. As shown in Table 1, 768 respondents completed the survey. Screening removed 75 surveys. The final sample was 693 surveys (or a 3.5 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	19,811	100.0%
Total returns	768	3.9%
Rejected or screened surveys	75	0.4%
Final sample	693	3.5%

We calculated a margin of error for all statistical survey questions that yielded a proportional or percentage result. Most questions utilized the full sample size of n = 693 qualified respondents. Assuming a confidence level at the 95 percent level, the margin of error for survey questions ranged from ± 1.0 percent to ± 6.9 percent, with an overall average of ± 4.1 percent.

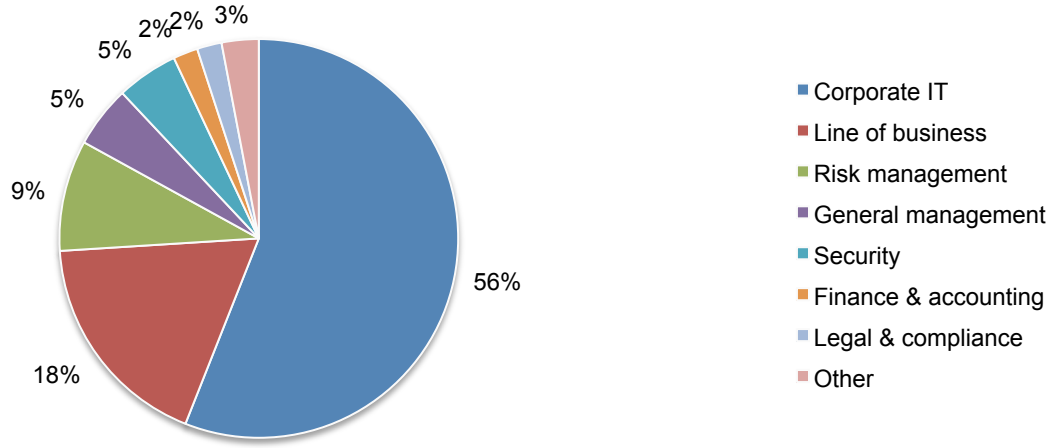
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (54 percent) reported their current position as supervisory or above.

Pie Chart 1. Current position or organizational level



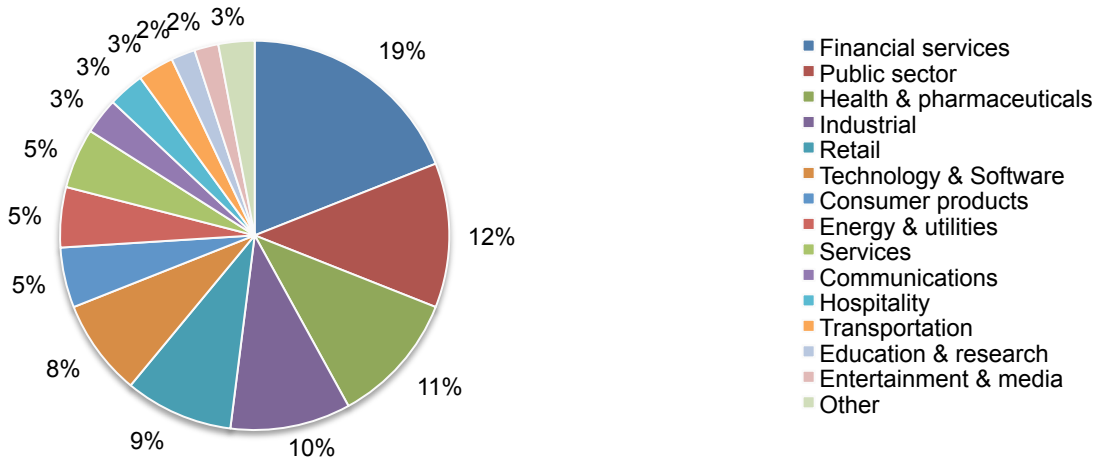
Pie Chart 2 identifies the department or function within the organization where the respondent is located. Fifty-six percent of respondents identified corporate IT and 18 percent responded line of business.

Pie Chart 2. The department or function where you are located in your organization



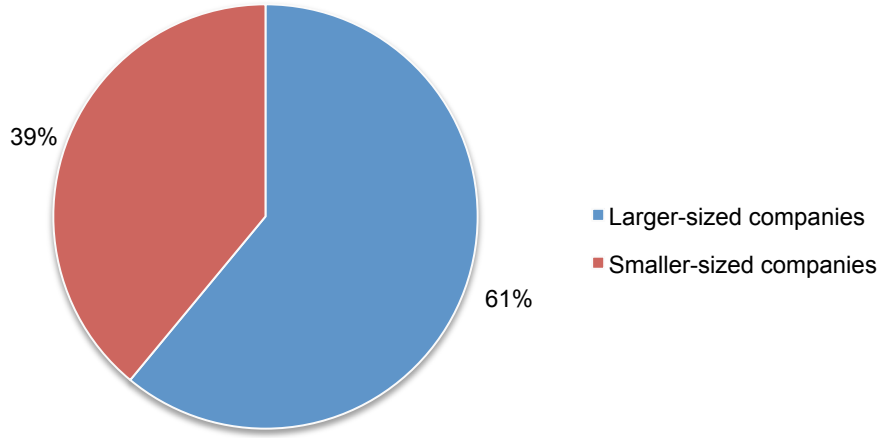
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (12 percent) and health and pharmaceuticals (11 percent).

Pie Chart 3. Primary industry focus



Pie Chart 4 shows the percentage of larger-sized companies that are members of the current Fortune 1,000, Forbes Global 2,000 and/or Forbes America's Largest Private Companies lists. Accordingly, 61 percent are large organizations and 39 percent are small organizations.

Pie Chart 4. Size of respondents' companies



Part 5. Caveats

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

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

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in various organizations in the United States. 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 specified time 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 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 2015.

Survey response	Freq	Pct%
Total sampling frame	19,811	100.0%
Total survey returns	768	3.9%
Rejected or screened surveys	75	0.4%
Final sample	693	3.5%

Part 1. Screening

S1. How familiar are you with threat intelligence collected and used by your company?	Pct%
Very familiar	33%
Familiar	44%
Somewhat familiar	23%
Not familiar (stop)	0%
Total	100%

S2. Does your company have one or more staff members dedicated to threat intelligence?	Pct%
Yes	100%
No (stop)	0%
Total	100%

S3. How are you involved in your company's cyber threat intelligence activities or process? Please select all that apply.	Pct%
User of threat intelligence	64%
Gatherer of threat intelligence	61%
Analyzer of threat intelligence	49%
Executive or manager in-charge of threat intelligence activities	35%
Not involved because we achieve good security without threat intelligence (stop)	0%

Part 2. General questions

Q1. How effective is your company's defense against cyber attacks? Please use the following scale from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	11%
3 or 4	19%
5 or 6	34%
7 or 8	26%
9 or 10	10%
Total	100%

Q2. How effective is your company's process for using actionable intelligence from **internal sources** (such as configuration log activities) to predict malicious IP activities? Please use the following scale from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	20%
3 or 4	21%
5 or 6	34%
7 or 8	19%
9 or 10	6%
Total	100%

Q3. How effective is your company's process for using actionable intelligence from **external sources** (such as vendor-supplied threat feeds) to predict malicious IP activities? Please use the following scale from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 or 2	35%
3 or 4	30%
5 or 6	20%
7 or 8	11%
9 or 10	4%
Total	100%

Q4. Do you believe gathering and using threat intelligence is essential to a strong security posture?	Pct%
Yes	53%
No	47%
Total	100%

Q5a. Does your organization use "free" sources of threat intelligence?	Pct%
Yes	55%
No	45%
Total	100%

Q5a. If yes, why? Please select all that apply	Pct%
Our organization does not have the budget to pay for threat intelligence	66%
There is not much difference between free and fee-based threat intelligence	36%
The free threat intelligence has proven to be effective in stopping security incidents	50%
Our organization uses both free and fee-based threat intelligence	39%
Other	1%

Q6a. Does your organization use "fee-based" sources of threat intelligence?	Pct%
Yes	49%
No	51%
Total	100%

Q6b. If yes, why does your organization pay for threat intelligence?	Pct%
Fee-based threat intelligence is better than free threat intelligence	80%
It has proven effective in stopping security incidents	76%
We don't have confidence in free sources of threat intelligence	25%
Free sources have not enabled our organization to prioritize threats	36%
Free sources have not been able to provide a comprehensive picture of the threat	51%
Other	1%

Q7. Typically, how is threat intelligence received by your organization? Please select all that apply.	Pct%
Data feeds from external sources	56%
Threat advisories	64%
Internal collection and analysis	71%
Exchange of threat intelligence with companies in the same industry	24%
Other (please specify)	2%

Q8a. Did your company have a material security breach in the past 24 months?	Pct%
Yes	40%
No	51%
Unsure	9%
Total	100%

Q8b. If yes, do you believe that threat intelligence could have prevented or minimized the consequences of the attack?	Pct%
Yes	80%
No	12%
Unsure	8%
Total	100%

Q9a. Typically, what threat intelligence does your company use? Please select all that apply.	Pct%
Threat indicators	64%
Software vulnerability patch updates	68%
Indicators of compromise	45%
Results of cybercrime investigations and prosecutions	23%
Other (please specify)	2%

Q9b. If you are using threat indicators, what information is most valuable? Please select all that apply.	Pct%
Indicators of malicious IP addresses	57%
Indicators of malicious malware	55%
Indicators of malicious URLs	46%
Indicators of malicious files	27%
Indicators of malicious mobile apps	50%
Suspicious phishing and spoofing sites	33%
Software vulnerability patch updates	67%
Indicators of compromise	45%
Other (please specify)	3%

Q10. Typically, how frequently does your organization receive threat intelligence?	Pct%
Real time	7%
Hourly	11%
Daily	25%
Weekly	6%
Bi-weekly	3%
Monthly	2%
On demand	29%
Other or irregular intervals	17%
Total	100%

Q11. Does the information you receive enable your organization to prioritize threats?	Pct%
Yes, most of the time	9%
Yes, some of the time	28%
No, rarely	32%
No, never	31%
Total	100%

Q12a. How satisfied are you in the threat intelligence your organization is receiving?	Pct%
Very satisfied	13%
Satisfied	16%
Somewhat satisfied	33%
Not satisfied	38%
Total	100%

Q12b. [If not satisfied] What are the main reasons why you are not satisfied? Please select the top two.	Pct%
Information is not timely	54%
Information is not categorized according to threat type or attacker	12%
Information does not provide enough context to make it actionable	46%
Information does not provide adequate guidance on what to do	13%
Uncertainty about the accuracy of the threat intelligence	25%
Uncertainty about the trustworthiness of data sources	27%
Information does not provide a comprehensive picture of the threat	6%
Information is too complicated to ensure ease and speed of use	17%

Q13. What best describes how you disseminate threat intelligence throughout your organization? Please select all that apply.	Pct%
Automated alerts through email or text messages	68%
Automated feed to security infrastructure	63%
Automated posting to web portal	39%
Manual distribution or process	55%
Ad hoc (no formal system or process in-place)	27%
Other (please specify)	1%

Q14. In which areas of your security infrastructure are you applying threat intelligence? Please select all that apply.	Pct%
Human analysis	55%
DNS firewall	47%
Anti-virus/anti-malware solutions	71%
UTM and/or next generation firewalls	47%
Reputation feeds to intrusion detection or prevention systems	63%
SIEM and other network intelligence tools	45%
Big data analytics	12%
Other (please specify)	1%

Q15. In which areas of your security infrastructure are you realizing the most benefit from threat intelligence? Please select the top two choices.	Pct%
Human analysis	49%
DNS firewall	28%
Anti-virus/anti-malware solutions	38%
UTM and/or next generation firewalls	22%
Reputation feeds to intrusion detection or prevention systems	25%
SIEM and other network intelligence tools	33%
Big data analytics	5%
Total	200%

Q16. Approximately, how many cyber attacks that eluded traditional defenses have you been able to discover because of threat intelligence from internal and external sources?	Pct%
None	6%
1 to 25	23%
26 to 50	24%
51 to 100	16%
More than 100	6%
Unable to determine	25%
Total	100%

Q17. How would you describe the trend in the amount of intelligence data your organization has consumed over the past 12 months?	Pct%
Increasing	45%
Decreasing	8%
Staying the same	35%
Unable to determine	12%
Total	100%

Q18. How accurate is the intelligence received by your organization? Please use the following scale from 1 = unreliable to 10 = very reliable.	Pct%
1 or 2	15%
3 or 4	36%
5 or 6	28%
7 or 8	12%
9 or 10	9%
Total	100%

Q19. How timely is the intelligence received by your organization? Please use the following scale from 1 = unreliable to 10 = very reliable.	Pct%
1 or 2	33%
3 or 4	28%
5 or 6	19%
7 or 8	12%
9 or 10	8%
Total	100%

Q20. How actionable is the intelligence received by your organization? Please use the following scale from 1 = not actionable to 10 = very actionable.	Pct%
1 or 2	29%
3 or 4	27%
5 or 6	18%
7 or 8	15%
9 or 10	11%
Total	100%

Q21. Who is **most** responsible for deciding what threat intelligence sources are used?	Pct%
Chief Information Officer	15%
Chief Technology Officer	9%
Chief Financial Officer	2%
Chief Information Security Officer	24%
Chief Risk Officer	10%
Line of business senior management	22%
Shared responsibility	18%
Other (please specify)	0%
Total	100%

Q22. Please check **one** statement that best describes how threat intelligence is exchanged within your organization.	Pct%
Centralized control within IT	24%
Centralized control within non-IT business function	21%
Centralized control by a dedicated team	30%
Decentralized control by a dedicated team	1%
Decentralized control within the line of business	24%
Other (please specify)	0%
Total	100%

Q23. What features make threat intelligence actionable? Please rank the following features from 1 = most important to 7 = least important.	Average	Rank
Timely	1.68	1
Trustworthiness of the source	2.20	3
Relevance to my industry	4.57	6
Ability to prioritize	3.33	4
Clear guidance on how to resolve the threat	6.19	7
Sufficient context	3.51	5
Ability to implement the intelligence	2.04	2

Q24. In general, when does threat intelligence become stale or not timely?	Pct%
Within seconds	21%
Within minutes	35%
Within hours	25%
Within days	8%
Within weeks	6%
Within months	5%
Other (please specify)	0%
Total	100%

Q25. What objective is most important to your organization's threat intelligence activities?	Pct%
To prevent attacks	33%
To quickly detect attacks	32%
To improve incident response	17%
All are equally important	18%
Total	100%

Q26. How confident are you in the security of sending your organization's threat intelligence data to the cloud for analysis (i.e., log files)?	Pct%
Very confident	11%
Confident	12%
Somewhat confident	25%
No confidence	47%
Unsure	5%
Total	100%

Part 3. Budget questions

Q27. Approximately, what range best defines your organization's current year budget for all IT operations? Please include licensing and maintenance fees, labor costs, investments in enabling technologies and overhead in your estimate.	Pct%
< $1 million	1%
$1 to $5 million	5%
$6 to $10 million	16%
$11 to $50 million	23%
$51 to $100 million	25%
$101 to $250 million	18%
$251 to $500 million	7%
> $500 million	5%
Total	100%

Q28. Approximately, what percentage of the current year's IT budget is allocated to IT security activities?	Pct%
< 1%	0%
1% to 2%	23%
3% to 5%	32%
6% to 10%	25%
11% to 15%	11%
16% to 20%	5%
21% to 30%	1%
31% to 40%	2%
41% to 50%	1%
> 50%	0%
Total	100%

Q29. Approximately, what percentage of the current year's IT security budget will go to activities relating to threat intelligence operations (both internal and external combined?	Pct%
< 1%	1%
1% to 2%	12%
3% to 5%	21%
6% to 10%	29%
11% to 15%	29%
16% to 20%	3%
21% to 30%	2%
31% to 40%	2%
41% to 50%	1%
> 50%	0%
Total	100%

Q30. How has your organization's budget or spending levels on threat intelligence changed over the past two years?	Pct%
Significant increase (> 20%)	19%
Increase	22%
No change	47%
Decrease	8%
Significant decrease (< 20%)	4%
Total	100%

Q31. In your opinion, how will your organization's budget or spending levels on threat intelligence change over the next two years?	Pct%
Significant increase (> 20%)	34%
Increase	33%
No change	24%
Decrease	7%
Significant decrease (< 20%)	2%
Total	100%

Part 4. Attributions: Please rate each of the following statements using the agreement scale below each item.	
Q32. The use of threat intelligence provides benefits that outweigh cost.	Pct%
Strongly agree	34%
Agree	33%
Unsure	18%
Disagree	11%
Strongly disagree	4%
Total	100%

Q33. Organizations need a real-time, machine-to-machine way to consume intelligence.	Pct%
Strongly agree	35%
Agree	33%
Unsure	19%
Disagree	10%
Strongly disagree	3%
Total	100%

Q34. Real-time reputation intelligence is an effective way to detect and respond to malicious IPs the moment they appear within our infrastructure.	Pct%
Strongly agree	29%
Agree	31%
Unsure	21%
Disagree	13%
Strongly disagree	6%
Total	100%

Q35. Continual monitoring and tracking of changes in IPs, URLs, files and mobile apps in real-time is essential to decreasing security incidents.	Pct%
Strongly agree	25%
Agree	29%
Unsure	24%
Disagree	14%
Strongly disagree	8%
Total	100%

Q36. Monitoring the good and bad of IPs, URLs, files and mobile apps that are related to an unknown object is an effective way to predict if they are to pose a security risk.	Pct%
Strongly agree	25%
Agree	28%
Unsure	30%
Disagree	9%
Strongly disagree	8%
Total	100%

Q37. Our organization receives too many alerts and false positives to make it possible to understand and respond to new threats.	Pct%
Strongly agree	31%
Agree	37%
Unsure	15%
Disagree	15%
Strongly disagree	2%
Total	100%

Part 5. Role and organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	1%
Director	17%
Manager	20%
Supervisor	15%
Technician	34%
Staff	5%
Contractor	4%
Other	2%
Total	100%

D2. Check the department or function that best describes where you are located in your organization.	Pct%
General management	5%
Finance & accounting	2%
Legal & compliance	2%
Corporate IT	56%
Line of business	18%
Human resources	0%
Risk management	9%
Security	5%
Other	3%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food service	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	19%
Health & pharmaceuticals	11%
Hospitality	3%
Industrial	10%
Logistics	1%
Public sector	12%
Retail	9%
Services	5%
Technology & Software	8%
Transportation	3%
Other	0%
Total	100%

D4. Where are your employees located? Please choose all that apply.	Pct%
United States	100%
Canada	66%
Europe	65%
Middle east & Africa	49%
Asia-Pacific	54%
Latin America (including Mexico)	51%

D5. Is the respondent's company a member of the current *Fortune 1000, Forbes Global 2000* and/or *Forbes America's Largest Private Companies* list?	Pct%
Larger-sized companies	61%
Smaller-sized companies	39%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

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

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