Ponemon INSTITUTE

Live Threat Intelligence Impact Report 2013

Sponsored by

NORSE

Independently conducted by Ponemon Institute LLC
Publication Date: July 2013

Contents

PART 1: INTRODUCTION

Executive Summary

Welcome to the Ponemon Institute Live Threat Intelligence Impact Report 2013. This comprehensive study of 708 respondents from 378 enterprises reveals the financial damage that slow, outdated and insufficient threat intelligence is inflicting on global enterprises and how live threat intelligence provides the ability to better defend against compromises, breaches and exploits.

Today's headlines and a barrage of marketing content lead many enterprise IT security and risk professionals to conclude that common cybercriminal tactics such as phishing attacks, malware and stolen credentials are responsible for the majority of breaches and compromises taking place.

While enterprises certainly need to defend against these attack vectors, this research reveals the connection between thwarting compromises and the need to have access to the most immediate threat intelligence available, or what is becoming known as "live threat intelligence." The research also shows that enterprises experiencing the highest number of compromises and breaches are reliant on slow, outdated and insufficient intelligence.

The findings in this report lead to a number of conclusions that will help security and risk professionals reduce the risk of breaches and compromises within the enterprises they are responsible for defending. These conclusions highlight the value of immediate threat intelligence, the current state of threat intelligence, the importance of live threat intelligence and the propensity enterprises have to invest in live intelligence solutions.

Glossary of key terms

The following terms are used throughout this report:

- **Live Cyberthreat Intelligence** refers to intelligence data about actual cyber attacks happening now; data is delivered with no delay. In contrast, "real-time" refers to the capture of data that is delivered with a short delay ranging from minutes to weeks after the event.
- **Dark Intelligence** refers to information gathered from places on the Internet where bad actors are found, such as proxies and honeypots.
- **Compromise or Security Breach** are terms used to describe an event that has exposed confidential data to unauthorized persons. A compromise can be either intentional or unintentional.
- **Data Breach** is a special case that specifically deals with exfiltration of sensitive or confidential information.
- **Security Attacks** occur when a person compromises a computer by installing harmful malicious software in the computer without the user's knowledge. This software includes viruses, spyware, worms and trojans.
- **Security Exploit** is an attack unleashed upon a single computer, network or enterprise system and based on a particular or known vulnerability.

While there are numerous key findings, the following were the most salient, revealing the impact that a lack of live threat intelligence is having on the enterprises represented in this research. According to respondents:

- $10 million is the average amount they spent in the past 12 months to resolve the impact of exploits.
- If they had actionable intelligence about cyberattacks within 60 seconds of a compromise, they could reduce this cost on average by $4 million annually (40 percent).
- Those that have been able to stop cyberattacks say they need actionable intelligence 4.6 minutes in advance to stop them from turning into compromises.
- Those not successful in detecting attacks believe 12 minutes is sufficient to stop them from turning into compromises.
- 60 percent said their enterprises were unable to stop exploits because of outdated or insufficient threat intelligence.
- 53 percent believe live intelligence is essential or very important to achieve a strong cybersecurity defense.
- 57 percent say the intelligence currently available to their enterprises is often too stale to enable them to grasp and understand the strategies, motivations, tactics and location of attackers.
- Only 10 percent know with absolute certainty that a material exploit or breach to networks or enterprise systems occurred.
- 23 percent said it can take as long as a day to identify a compromise.
- 49 percent said it can take within a week to more than a month to identify a compromise.

In addition to these findings, it is worth mentioning that while enterprises continue to invest heavily in traditional IT security solutions, the majority of respondents have mixed levels of confidence in their ability to provide effective defense. Enterprises are using a wide range of technologies to gather threat intelligence, ranging from SIEM to IDS to IAM and firewalls. However, on a scale of effectiveness, only 22 percent of respondents rate them between a seven and a ten, and 78 percent rate them between a one and a six.

“Ponemon Institute has conducted IT security research for over a decade, and this is one of the first studies that reveals the facts behind the impact that weak threat intelligence is having on organizations,” said Dr. Larry Ponemon, founder and chairman of Ponemon Institute. “Readers of this report will come to understand that live threat intelligence must be an integral part of any security strategy.”

The study surveyed 708 IT and IT security professionals in 378 organizations. These professionals ranged in position from executive vice president to staff, with technicians (35 percent) making up the largest respondent segment. Sixty percent of respondents report directly to the chief information officer.

Represented in this study are 14 industry segments, including financial services (19 percent of respondents) as the largest segment, followed by health and pharmaceutical (12 percent of respondents) and public sector (12 percent of respondents). Thirty percent of respondents work in enterprise-sized organizations with a global headcount of 5,000 or more employees.

PART 2: KEY FINDINGS

The value of immediate intelligence

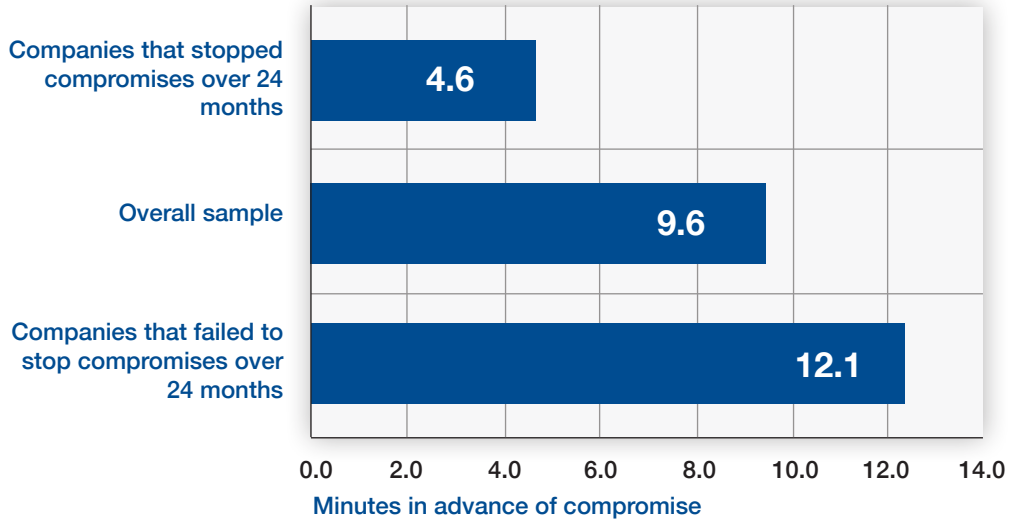
In this study, the companies that seem to be most successful in thwarting compromises to networks and enterprise systems are aware of the need to have the most immediate intelligence available. In other words, there is a "time/value" of actionable intelligence, according to this research.

As shown in Figure 1, companies that successfully stopped compromises say the optimal age of actionable intelligence is no longer than 4.6 minutes. In contrast, companies in this study that have a history of not being able to stop compromises are not as aware of the need for timely intelligence. Specifically, they believe 12.1 minutes is satisfactory. The average desired time for actionable intelligence, according to respondents, is 9.6 minutes.

Differences in estimated time thresholds support our proposition that speed is of the essence, especially for companies with a stronger security posture. Accordingly, the ability to quickly gather, analyze and use actionable intelligence is essential to cyber defense.

The ability to quickly gather, analyze and use actionable intelligence is essential to cyber defense.

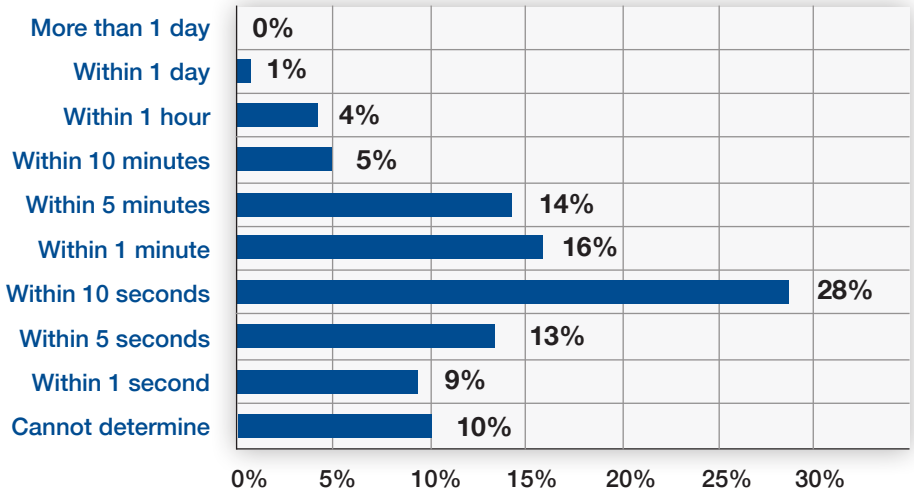
FIGURE 1 **How many minutes of advance warning do you need?**



The current state of cyber threat intelligence

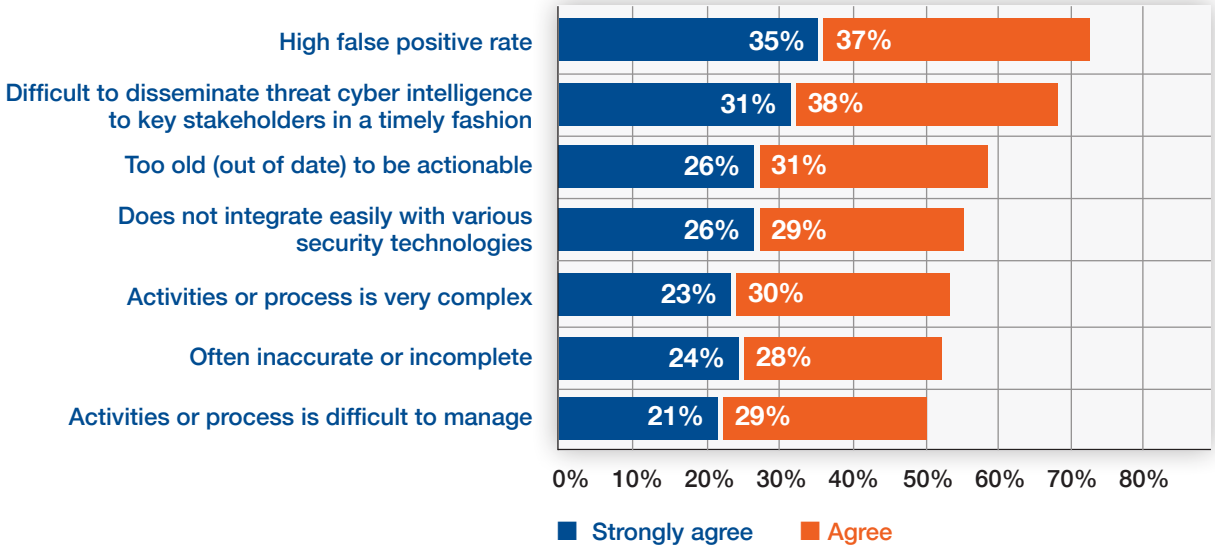
Cyber threat intelligence is often too old to be actionable. On average, respondents say at the very minimum they need on average about 10 minutes in order to prevent a compromise to networks or enterprise systems, as shown in Figure 2. However, most respondents (57 percent) say the intelligence they depend upon to protect their companies is often too old to be actionable.

FIGURE 2 **Time in advance of a cyber attack needed to prevent a compromise**
Extrapolated average is 9.6 minutes



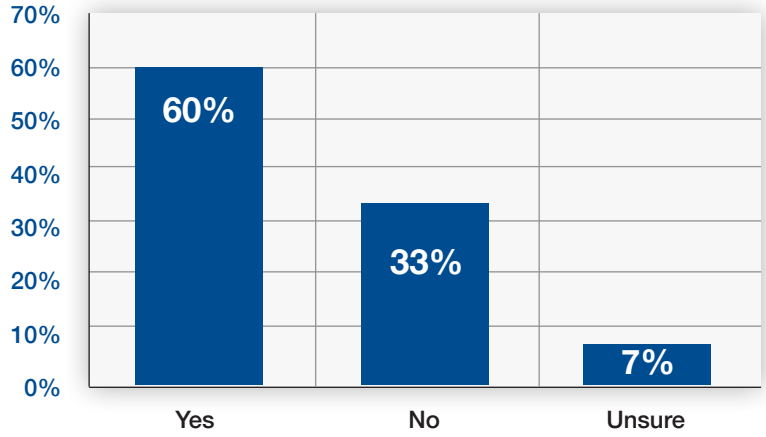
Respondents believe there are other reasons for the ineffectiveness of current intelligence. Specifically, cyber threat intelligence has a high false positive rate and it is difficult to share the intelligence in a timely manner with key stakeholders, as revealed in Figure 3.

FIGURE 3 **Perceptions about problems with cyber threat intelligence**
Strongly agree and agree response combined



Security exploit failures are often unstoppable due to outdated intelligence. The findings of this research clearly indicate that companies need to improve their ability to detect and respond to cyber security attacks. Sixty percent of respondents agree that their company at some point in time failed to stop a material security exploit because of insufficient or outdated threat intelligence, as shown in the "yes" response in Figure 4. Thirty-three percent say that poor intelligence is not a factor and 7 percent are unsure.

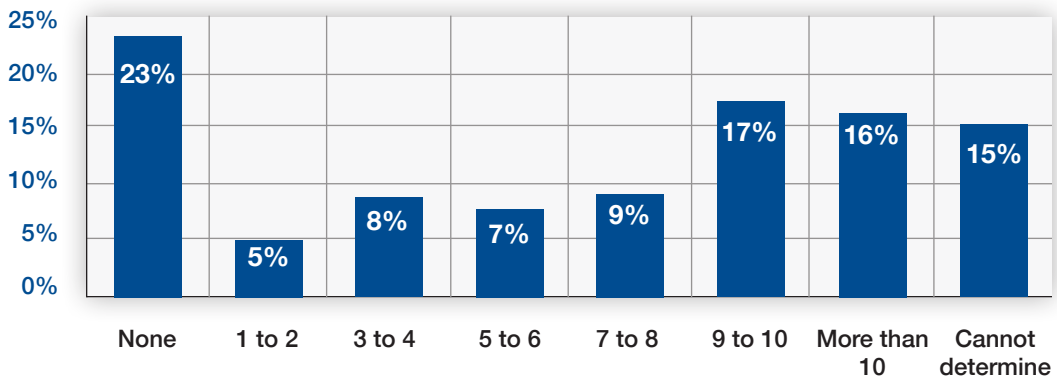
FIGURE 4 **Was the company *unable to stop* a security exploit because of outdated or insufficient intelligence?**



Respondents say multiple security exploits were not stopped because organizations did not have the necessary advance warnings and intelligence. Figure 5 reports the number of security exploits experienced by respondents' companies over the past 24 months. Please note that this figure only shows results for 60 percent of respondents (see Figure 4) who say their companies experienced one or more incidents – some happening more than two years earlier.

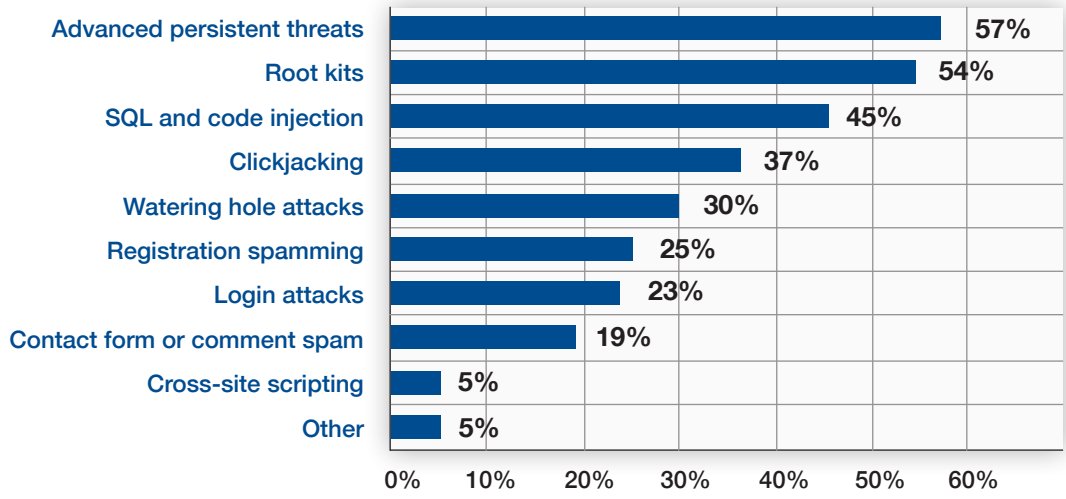
A further analysis presented in Figure 5, reveals that 23 percent record zero failures in the past two years. Sixty-two percent say they failed to prevent one or more security exploits in the past two years. One-third (17+16) percent of respondents say their organizations failed to stop 9 or more security exploits over two years. On average, companies experienced approximately six such exploits in the past two years that could not be stopped because of intelligence failures.

FIGURE 5 **Number of security exploits not stopped because of outdated intelligence**
Extrapolated average 5.7 failed to be prevented



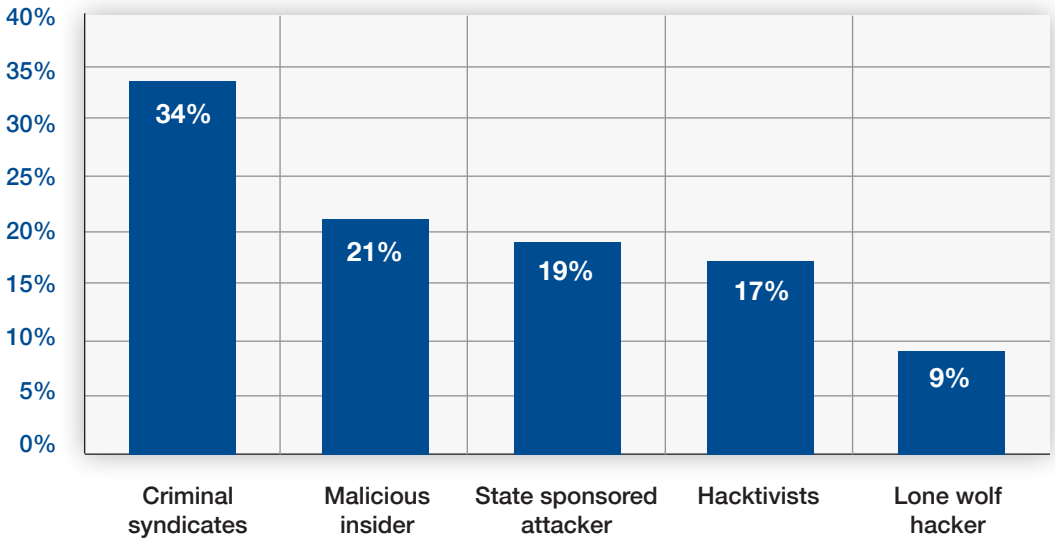
Certain threats and attackers are considered more serious than others. According to Figure 6, the most serious types of cyber attacks are advanced persistent threats (APT), root kits and SQL and code injection.

FIGURE 6 **The most serious types of cyber attacks**
Three choices permitted



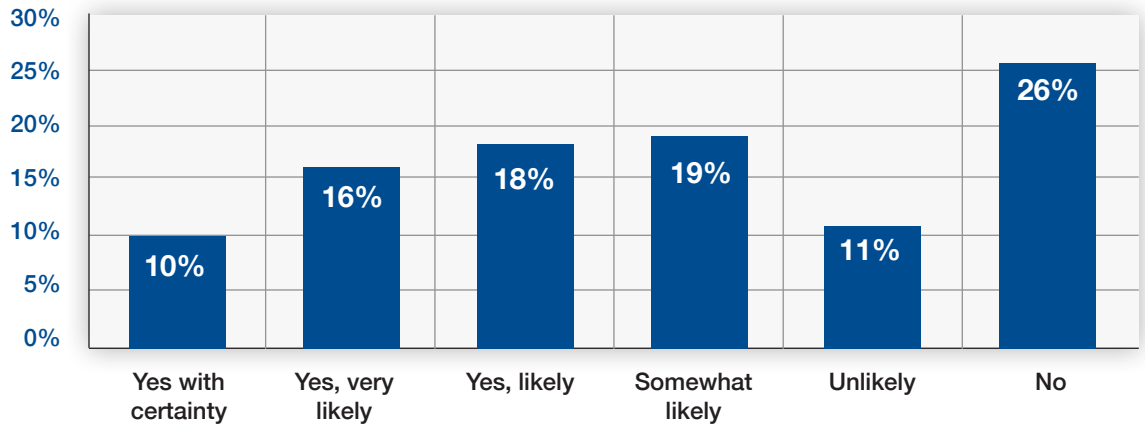
The most lethal attackers are the criminal syndicates and malicious insider followed by those that are state sponsored, as shown in Figure 7.

FIGURE 7 **Most threatening cyber attacker**



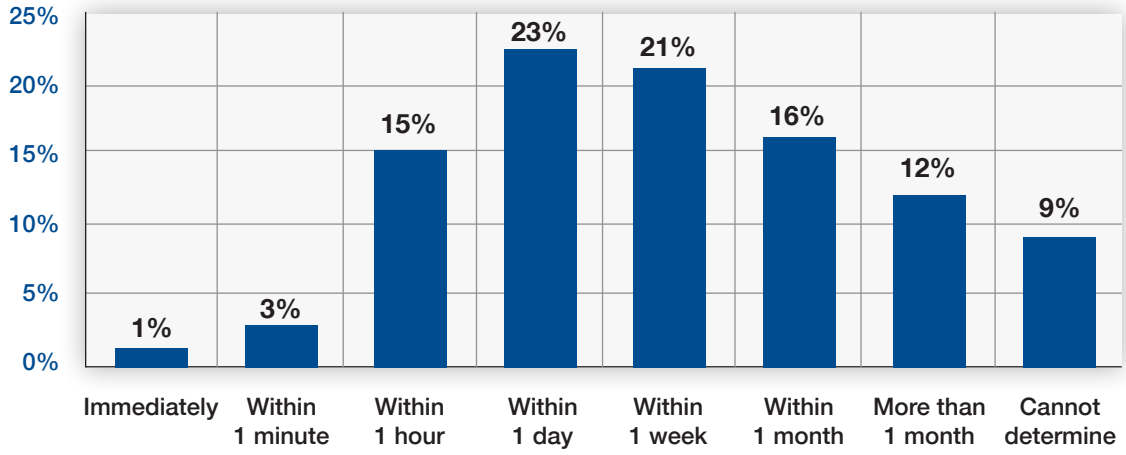
Breaches and security exploits often go undetected. As previously discussed, the cyber intelligence available to companies is often inadequate and outdated. The lack of knowledge about when and if their company's website, networks or enterprise systems are compromised puts organizations at great risk. Figure 8 reveals that 37 percent say either no (26 percent) or it would be unlikely (11 percent) to know about such an exploit. Only 10 percent say they would know with certainty if such an incident occurred.

FIGURE 8 **Awareness of a website, network or enterprise system compromise**



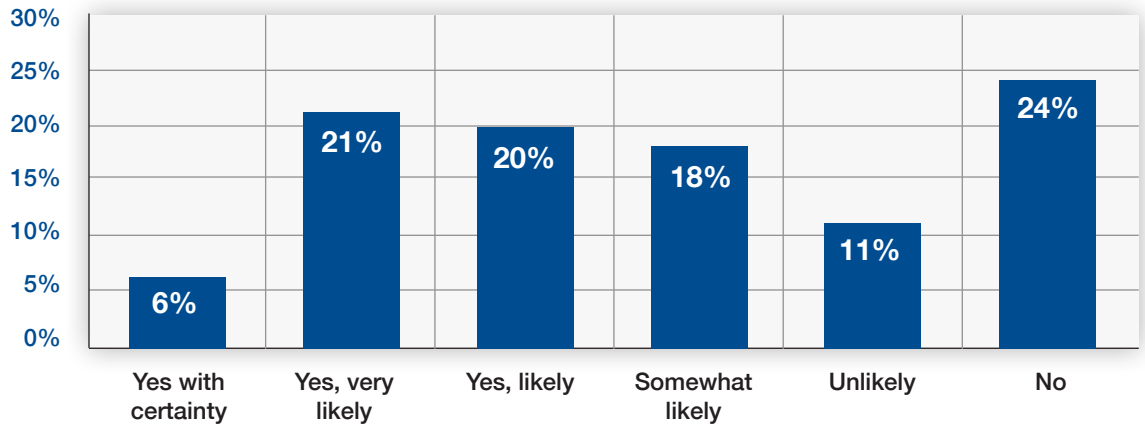
If detection is possible, respondents say it would take on average approximately 11 days to know with a high degree of certainty, according to Figure 9.

FIGURE 9 **How long before knowing with certainty that a compromise has occurred**
Extrapolated average 10.9 days



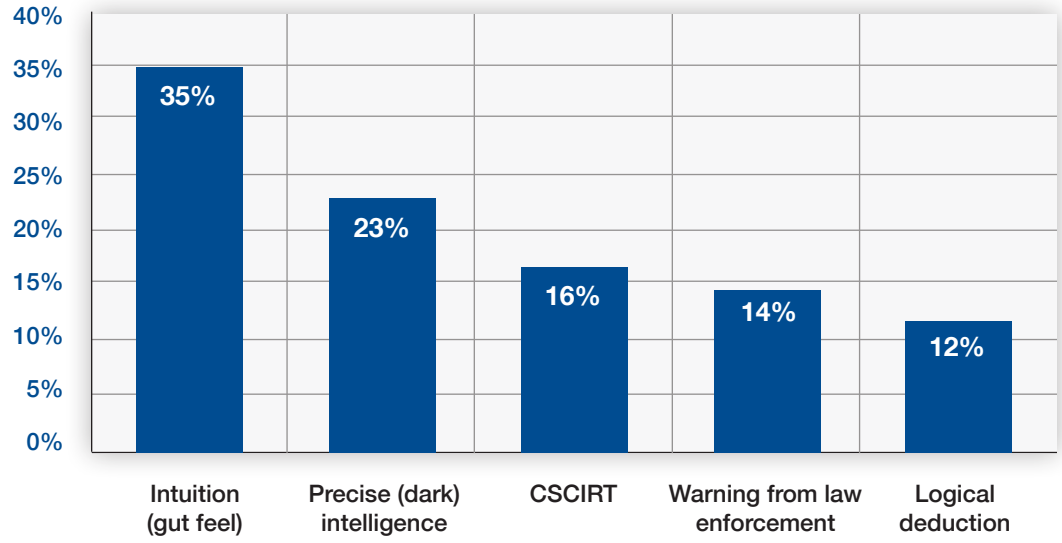
Most respondents believe their organization is a target. According to Figure 10, 65 percent of respondents do believe either with certainty or with some likelihood that their company has been targeted for attack. Only 35 percent believe it is unlikely that their organization is targeted (11 percent) or not targeted (24 percent).

FIGURE 10 **Is your organization targeted for an attack?**



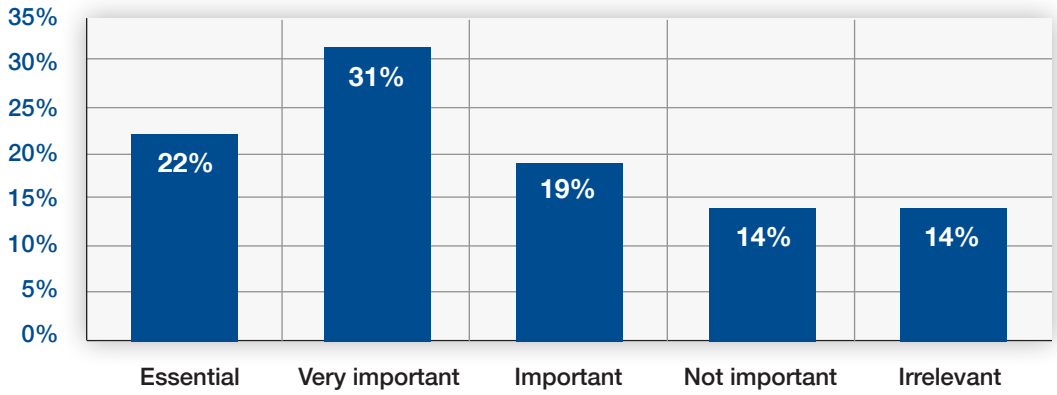
Is this belief based on intelligence that can help them stop the attack? Thirty-five percent of respondents say they are relying upon intuition or gut feel, as shown in Figure 11. Only 23 percent say their organizations rely upon precise intelligence.

FIGURE 11 **How do you know an attack will occur?**



While the majority of respondents (53 percent) believe it is essential or very important to know the geo-location for determining the severity of cyber threats (Figure 12), 44 percent of respondents are not certain about the geo-location or origin of cyber attacks that target their company. Only 33 percent are very certain or certain they have this information.

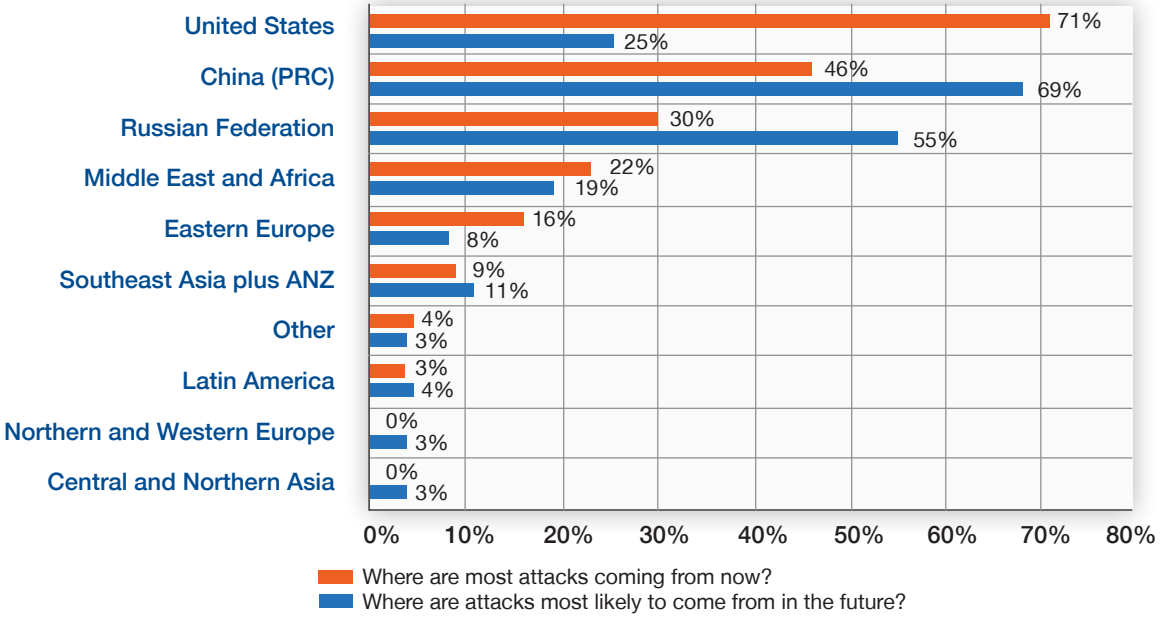
FIGURE 12 **The importance of geo-location for determining the severity of cyber threats**



Sixty-one of all respondents say they did not know the origin of cyber attacks experienced by them in the recent past. Responses from the remaining 39 percent are analyzed in Figure 13.

The figure summarizes the origin of cyber attackers. In terms of recent past incidents, it appears that cyber attacks were most likely to originate in the U.S., followed by China and the Russian Federation. With respect to future attacks, however, respondents believe attacks are most likely to originate in China and Russia. As can be seen, attacks launched from the U.S. are projected to decline to third place.

FIGURE 13 **Origin of cyber attacks**
Two responses permitted

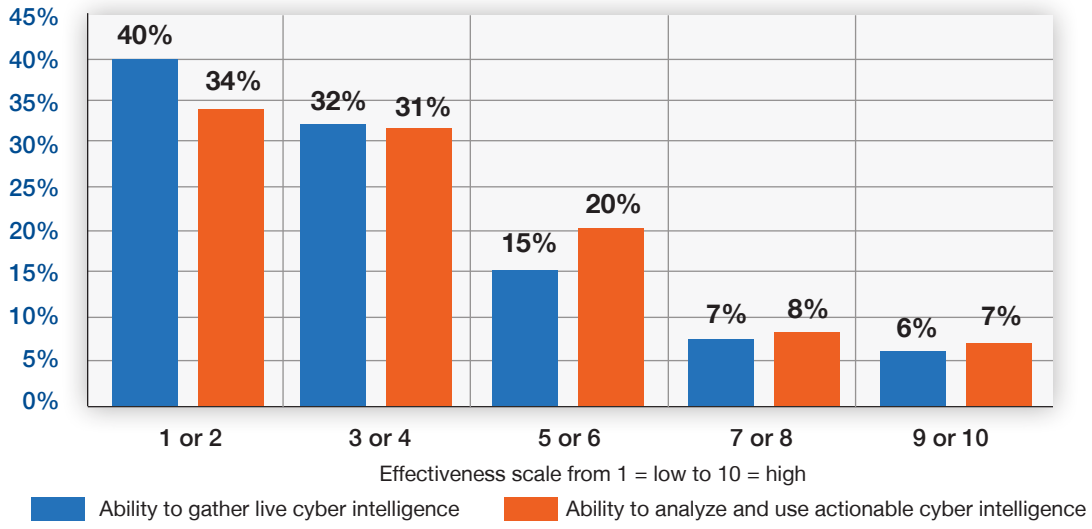


The importance of live intelligence

In the context of this research, live refers to intelligence data about actual cyber attacks happening now without any delay. In contrast, "real-time" refers to the capture of data with a short delay that ranges from minutes to weeks after the event.

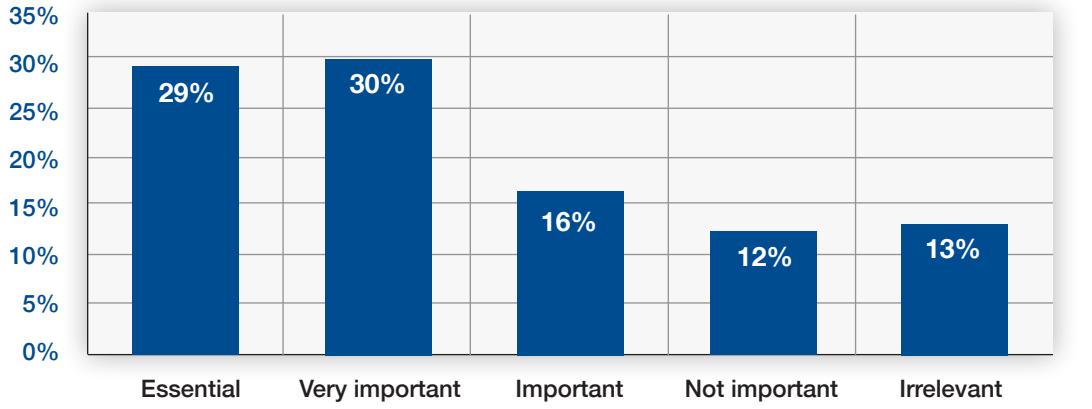
Respondents give their companies low marks for gathering and analyzing live intelligence. Sixty-three percent of respondents say live intelligence is essential or very important to achieving a strong cybersecurity defense. However, they rate their ability to gather live cyber intelligence very low (an average of 3.6 on a scale of 1 to 10) and to analyze and use actionable cyber intelligence equally low (an average of 4 on a scale of 1 to 10), according to Figure 14.

FIGURE 14 **Effectiveness of the ability to gather and analyze cyber intelligence**



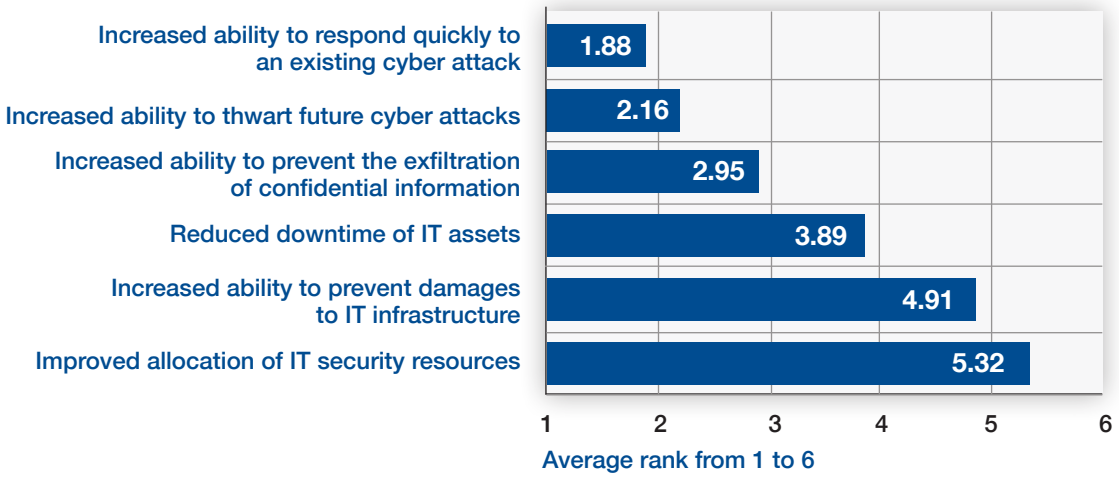
How would respondents change their approach to dealing with cybersecurity threats? The majority of respondents (59 percent) consider the use of big data analytics as essential or very important to achieving a strong cyber security defense, as shown in Figure 15.

FIGURE 15 **The importance of big data analytics to a strong cyber security defense**



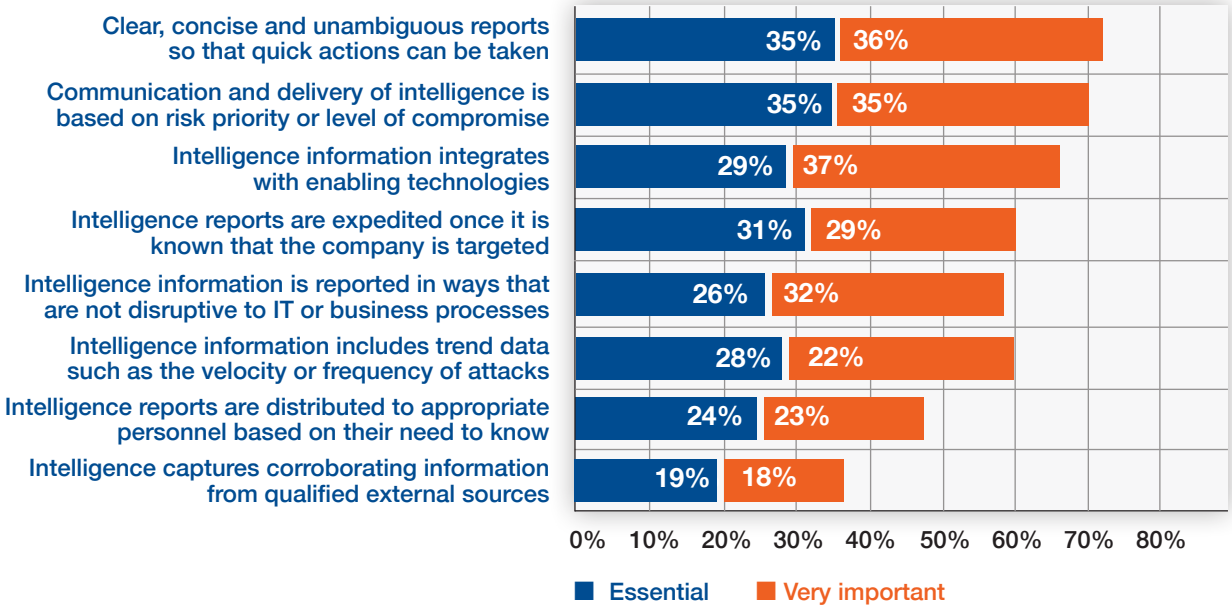
According to Figure 16, the most important metrics to assess the value of live intelligence are increased ability to respond quickly to an existing cyber attack, thwart future cyber attacks and prevent the exfiltration of confidential information.

FIGURE 16 **Average rank of metrics on the value of live intelligence**
1 = most important to 6 = least important



There are seven features of security solutions that are considered essential or very important to deal with security exploits. As shown in Figure 17, the availability of reports prepared in a way that enables quick response and based on the seriousness of the risk is most critical. These features are followed by compromise solutions that integrate with enabling technologies such as SIEM or other network monitoring tools.

FIGURE 17 **Enabling security features that make reports more actionable and useful**
Essential and very important response combined

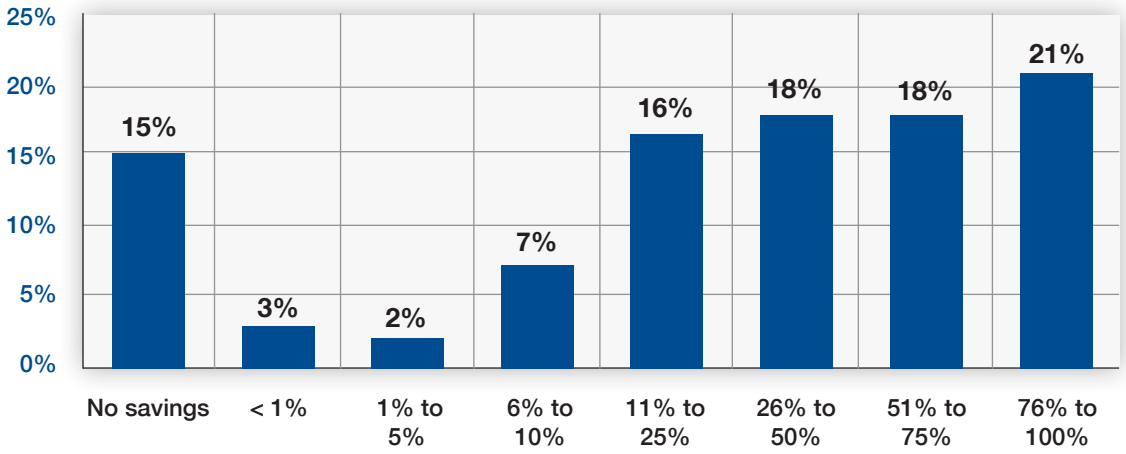


The budget for IT security and live intelligence

We asked respondents to estimate the cost of cyber exploits experienced over the past 12 months. These costs include all out-of-pocket expenses, productivity impact, legal costs and reputational damages.

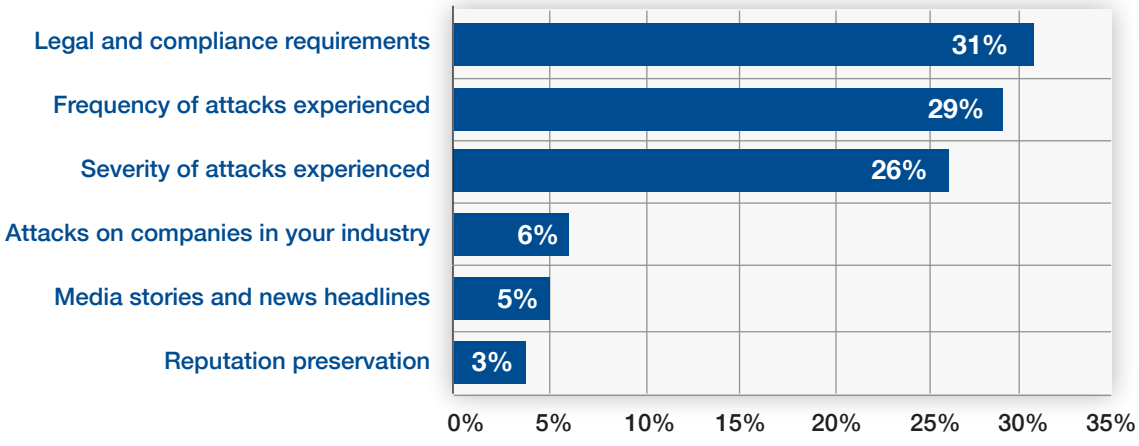
The cost of cyber attacks can be reduced by live intelligence. On average, companies represented in this study spent more than $10 million to resolve the impact of cyber exploits. However, they believe that if they had actionable intelligence of cyber attacks within 60 seconds of a compromise they could reduce the cost on average by 40 percent or by more than $4 million as revealed in Figure 18.

FIGURE 18 **Savings if intelligence is received within 60 seconds before a cyber attack**
Extrapolated savings 40 percent



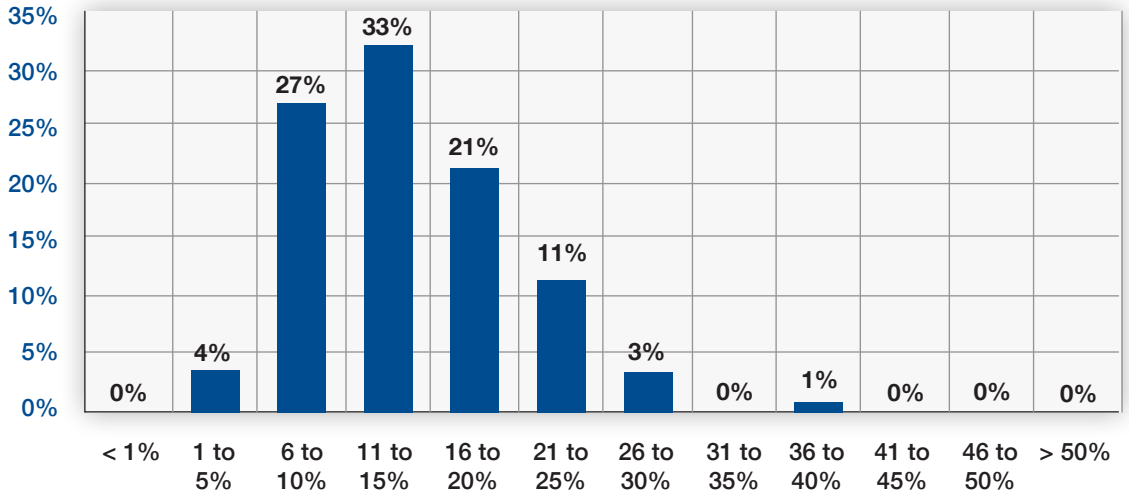
The main driver of security spending is compliance. According to Figure 19, 31 percent of respondents say determination about how much to spend on IT security is based on legal and compliance requirements followed by the frequency and severity of the attacks.

FIGURE 19 **Determining factors for IT security budget**
One response permitted



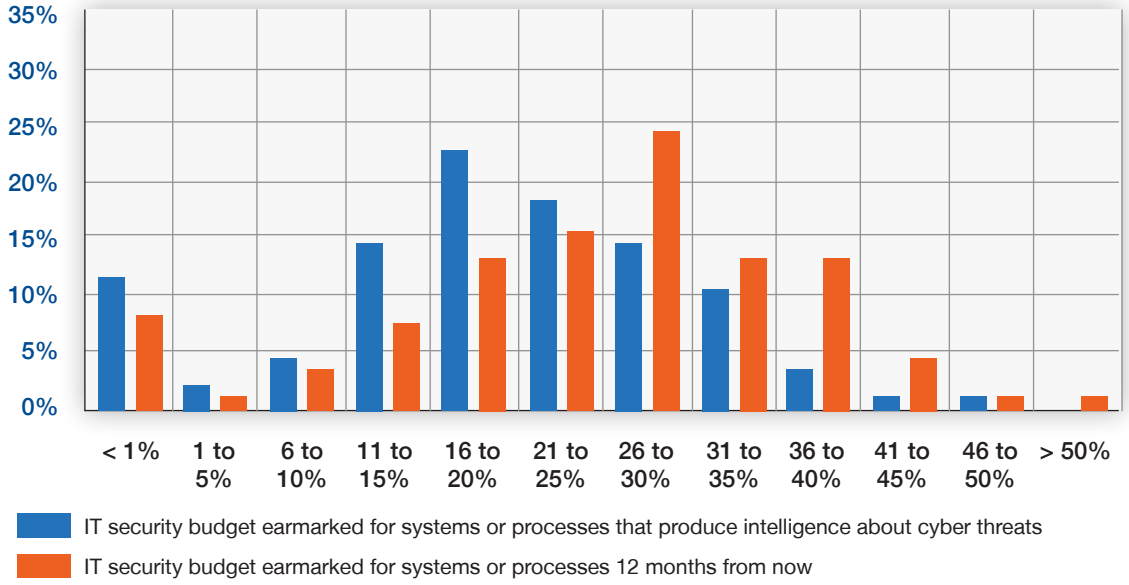
On average, companies spend about $95 million on IT and 14 percent of this is allocated to IT security as revealed in Figure 20.

FIGURE 20 **Allocation of budget dedicated to IT security**
Extrapolated average 14 percent



Currently the average budget earmarked for systems or processes that produce intelligence about cyber threats is 20 percent of the IT security budget or approximately $3 million as shown in Figure 21. This is expected to increase to $3.2 million or 25 percent of the average IT security budget in the next 12 months.

FIGURE 21 **Allocation of IT security budget**

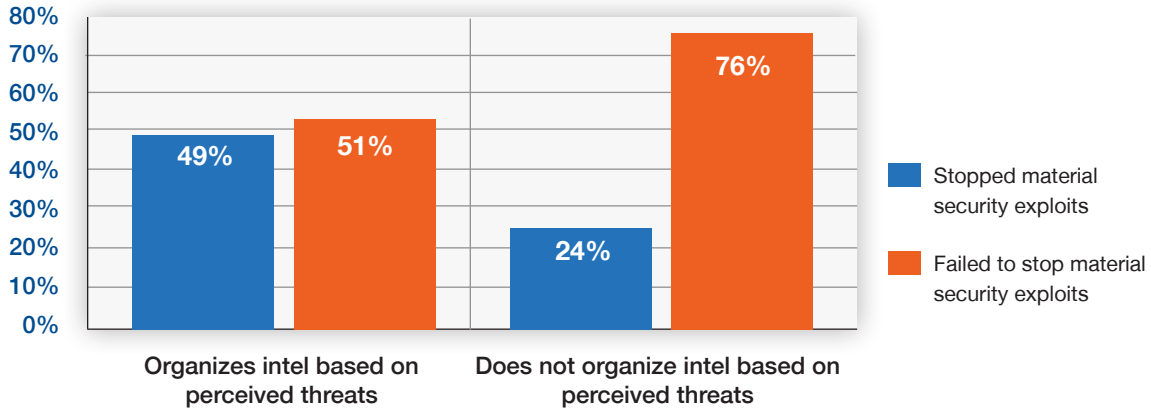


Special analysis: Live intelligence results in a stronger cyber security posture

Cross-tab analyses of certain findings reveal relationships between the use of live intelligence and a strong cyber security posture. We looked at companies that report they either organize or fail to organize actionable intelligence based on perceived threats.

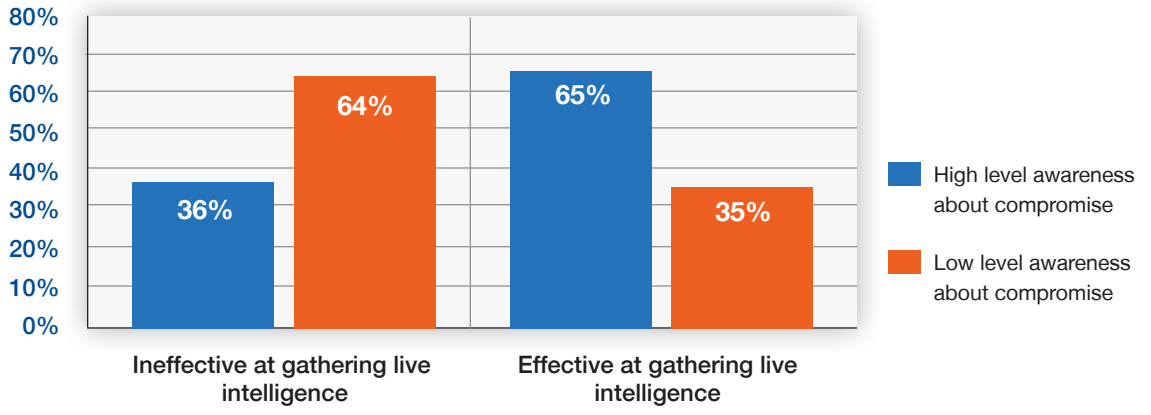
As reported in Figure 22, companies that organize intelligence based on perceived threats are much more likely to stop material security exploits (49 versus 24 percent). In contrast, companies that do not organize intelligence based on perceived threats are much less likely to stop material security exploits (76 versus 51 percent).

FIGURE 22 **Failed to stop a security exploit because of insufficient or outdated cyber threat intelligence**



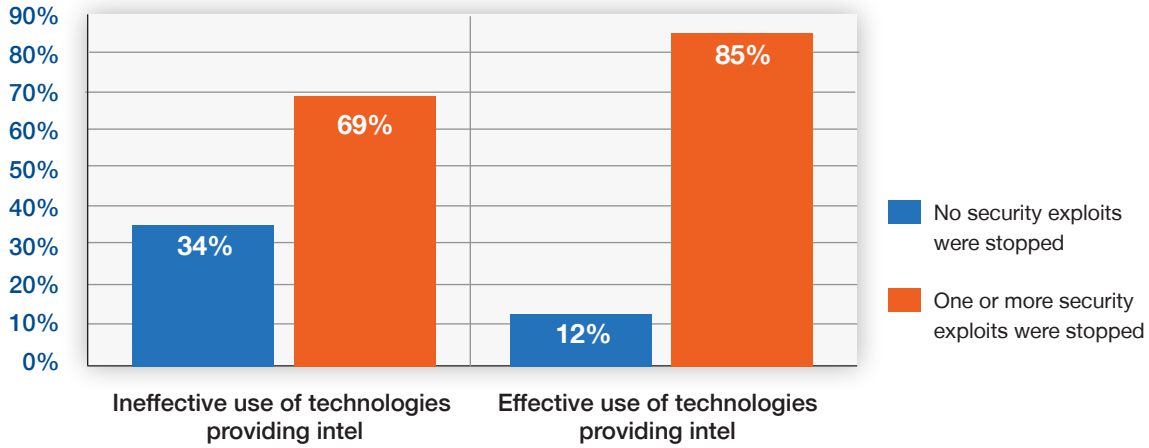
Companies that report they are effective in gathering live intelligence are more likely to know when their networks or systems are compromised. As shown in Figure 23, respondents who are effective at gathering live intelligence are more likely to have a high level of awareness about a network or system compromises (65 versus 35 percent). In contrast, respondents who are ineffective at gathering live intelligence are more likely to have a low level of awareness about network or system compromises (64 versus 36 percent).

FIGURE 23 **Awareness of a website, network or enterprise system compromise**



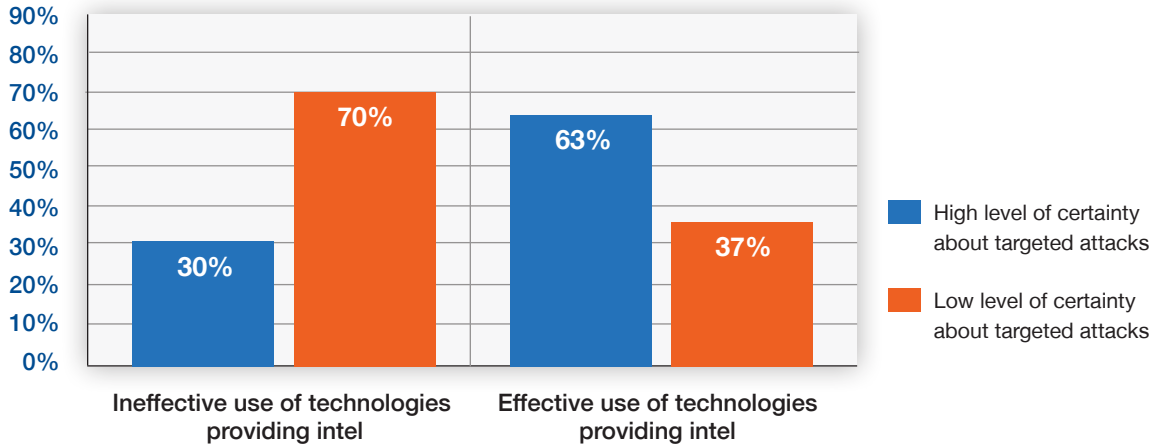
According to participants, availability of actionable intelligence is among the most important features of enabling security technologies. As shown in Figure 24, companies that are effectively using enabling technologies are more likely to have stopped one or more security exploits over the past 24 months (85 versus 69 percent). In contrast, companies that are ineffectively using enabling security technologies are more likely to state they have not stopped a security exploit over the past 24 months (34 versus 12 percent).

FIGURE 24 **Were security exploits stopped because of enabling technologies?**



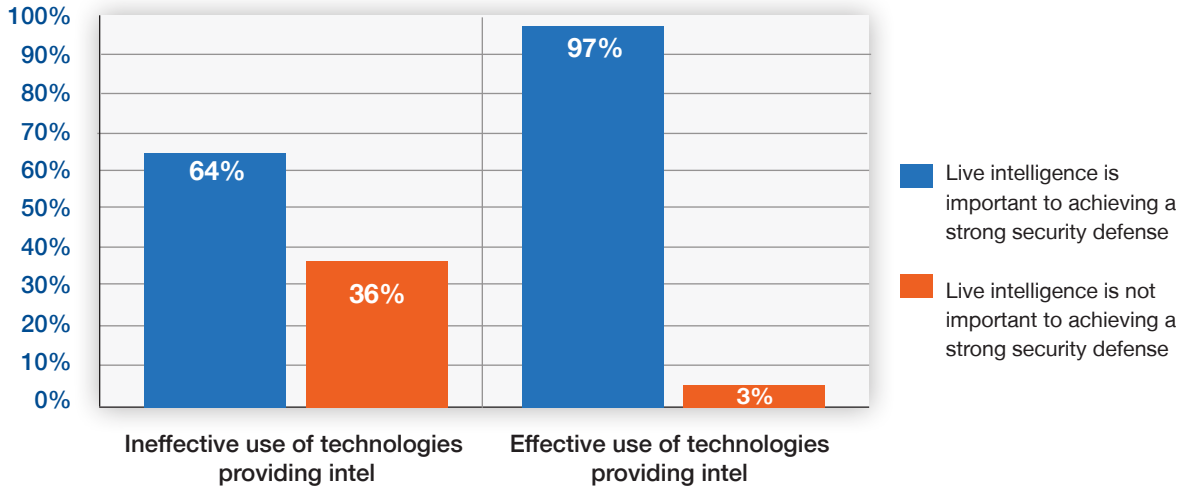
Knowing that cyber attackers have targeted your company is very important to a strong security defense. Our research shows companies that have actionable intelligence are more likely to recognize when they are at risk. As shown in Figure 25, over 70 percent of organizations that are ineffective users of enabling technologies are uncertain about being targeted by attackers. In contrast, 63 percent of organizations that are effective users of enabling technologies have a high level of certainty about being targeted. Taken together, this cross-tabulation suggests companies with the ability to capture actionable intelligence from enabling security technologies are more cognizant of being the subject of attacks such as advanced persistent threats.

FIGURE 25 **Is your company targeted by attackers?**



Companies that use technologies providing actionable intelligence are more likely to see their intelligence gathering activities as effective. The following cross-tabulation in Figure 26 shows 97 percent of organizations that are effective users of enabling security technologies, versus 64 percent of ineffective users, believe live intelligence is important to achieving a strong security defense.

FIGURE 26 **Importance of live intelligence in achieving a strong cyber security defense**



PART 3: CONCLUSION

This research reveals the value of having intelligence in enough time to stop a cyber attack. However, while timing can be everything, the completeness and relevancy of the intelligence is also critical.

According to the findings, the majority of respondents agree that it is hard to stop a compromise to networks or enterprise systems because the intelligence is out-of-date, inaccurate or incomplete. Further, there is often a high false positive rate that distracts from pursuing the real threats and attacks.

The combination of timely intelligence and quality reporting can improve an organization's ability to stop attacks. The majority of these professionals say the following seven features of cybersecurity reporting are critical:

The completeness and relevancy of the intelligence is critical.

1. Intelligence reports that are clear, concise and unambiguous so that quick actions can be taken.
2. Communication and delivery of intelligence is based on predetermined risk priorities or level of compromise.
3. Intelligence information integrates with enabling technologies such as SIEM or other network monitoring tools.
4. Intelligence reports are expedited once it is known that the company is being targeted.
5. Intelligence information is reported in ways that are not disruptive to IT operations or business processes.
6. Intelligence information includes trend data such as the velocity or frequency of attacks.
7. The use of big data analytics is also considered essential to a strong cybersecurity posture.

The benefits of having actionable intelligence include a stronger security posture and greater awareness about when a network or system has been compromised. Further, the study shows that the effective use of enabling technologies can lead to the prevention of security exploits and greater cognizance of the type of cyber attack.

PART 4: METHODS

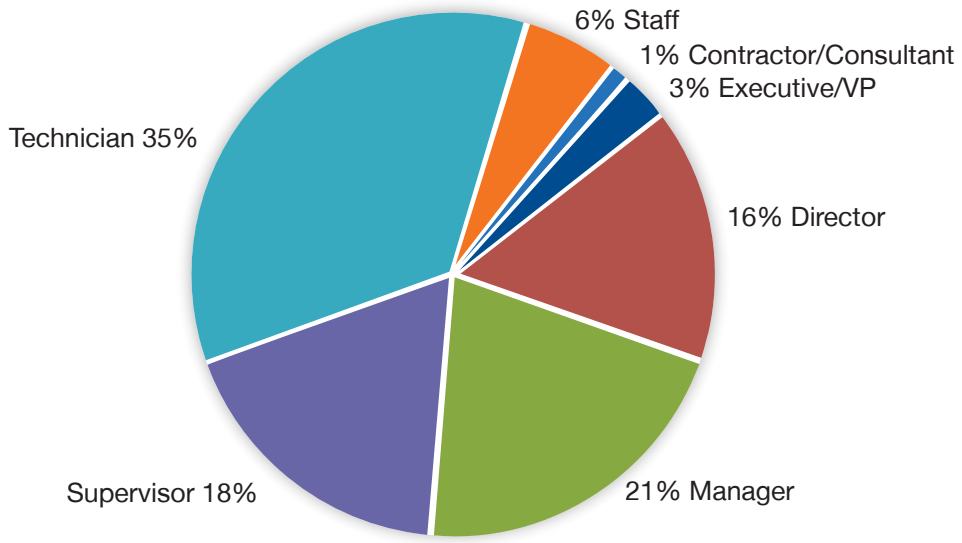
A random sampling frame of 18,700 IT or data security practitioners located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 832 respondents completed the survey. Screening and reliability checks removed 124 surveys. The final sample was 708 surveys (or a 3.8 percent response rate).

Table 1.

Sample response	Freq	Pct%
Sampling frame	18700	100%
Total returns	832	4.4%
Rejected and screened surveys	124	0.7%
Final sample	708	3.8%

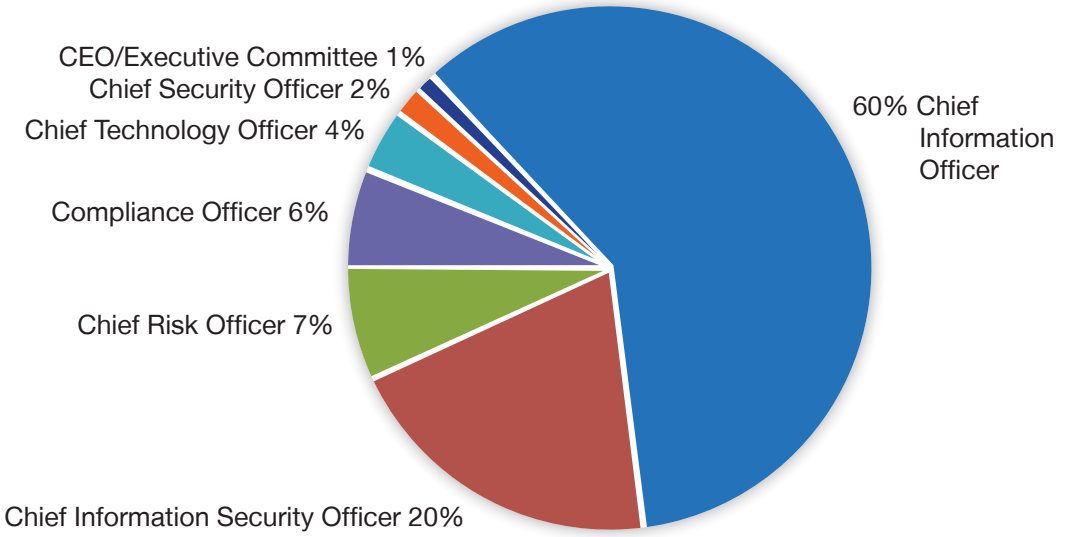
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 58 percent of respondents are at or above the supervisory levels.

PIE CHART 1. **Current position within the organization**



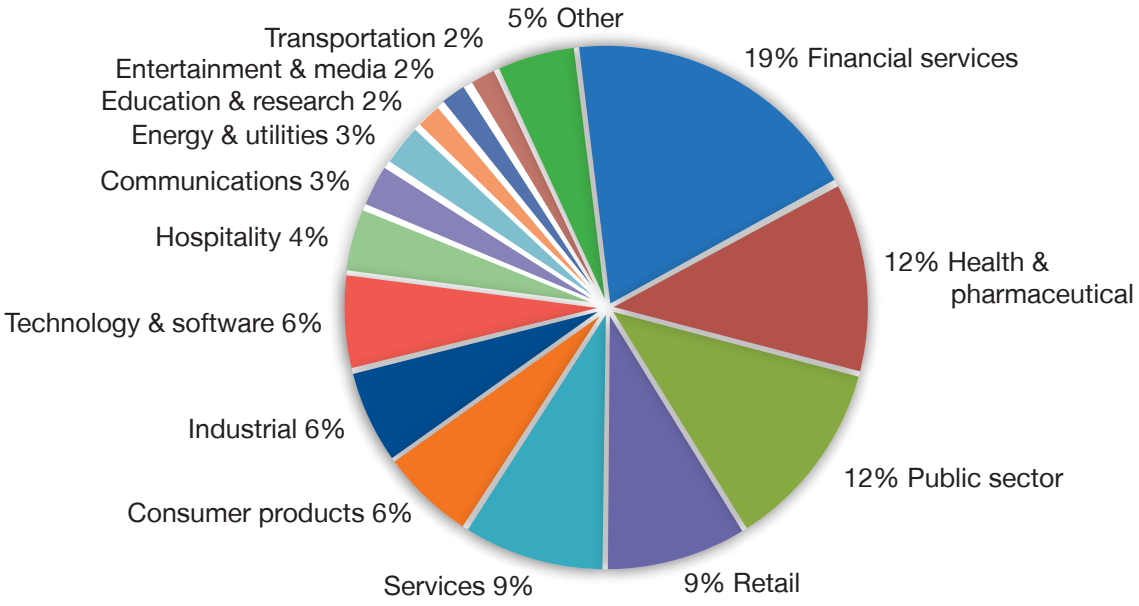
Pie Chart 2 shows 60 percent of respondents reporting directly to the Chief Information Officer and 20 percent reporting to the Chief Information Security Officer.

PIE CHART 2. The primary person you or the immediate supervisor reports to within the organization



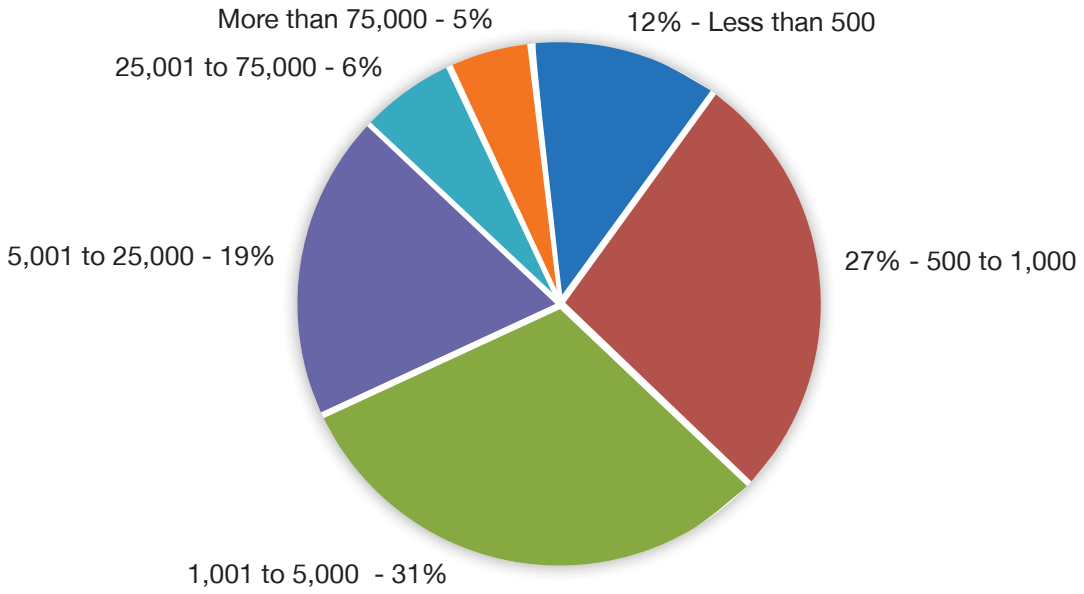
Pie Chart 3 reports a total of 14 industry segments of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceutical (12 percent) and public sector (12 percent),

PIE CHART 3. Industry distribution of respondents' organizations



As shown in Pie Chart 4, 61 percent of respondents are from enterprise-sized organizations with a global headcount of 1,001 or more employees. The remaining 39 percent represents small-tomedium sized (SMB) companies. At 31 percent, companies with a headcount between 1,001 to 5,000 full time equivalent employees represents the largest segment. The smallest segment, at 5 percent, pertains to organizations with headcount at more than 75,000 employees.

PIE CHART 4. **Worldwide headcount of the organization**



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. 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 in June 2013.

Sample response	Freq	Pct%
Sampling frame	18700	100%
Total returns	832	4.4%
Rejected and screened surveys	124	0.7%
Final sample	708	3.8%

Part 1. Screening

S1. How familiar are you with the cyber threat intelligence collected and used by your company?	Freq	Pct%
Very familiar	215	30%
Familiar	310	44%
Somewhat familiar	183	26%
Not familiar (stop)	0	0%
Total	708	100%

S2. How are you involved in your company's cyber threat intelligence activities or process? Please select all that apply.	Freq	Pct%
User of threat intelligence	402	57%
Gatherer of threat intelligence	291	41%
Analyzer of threat intelligence	326	46%
Executive or manager in-charge of threat intelligence activities	118	17%
None of these roles (stop)	0	0%
Total	1137	

Part 2. Attributions

Please rate the following statements using the five-point scale provided below each item.	Strongly Agree	Agree
Q1a. My company's cyber threat intelligence is often too old (out of date) to be actionable	26%	31%
Q1b. My company's cyber threat intelligence is often inaccurate or incomplete	24%	28%
Q1c. My company's cyber threat intelligence activities or process is very complex	23%	30%
Q1d. My company's cyber threat intelligence activities or process is difficult to manage	21%	29%
Q1e. My company's cyber threat intelligence has a high false positive rate	35%	37%
Q1f. It is difficult to disseminate threat cyber intelligence to key stakeholders in a timely fashion	31%	38%
Q1g. My company's cyber threat intelligence does not integrate easily with various security technologies	26%	29%

Part 3. Background

Q2. What is the minimum time necessary to have a material impact on your company's ability to prevent a compromise to networks or enterprise systems? In other words, how much time in advance of a cyber attack do you really need to prevent a compromise?	Pct%
Within 1 second	9%
Within 5 seconds	13%
Within 10 seconds	28%
Within 1 minute	16%
Within 5 minutes	14%
Within 10 minutes	5%
Within 1 hour	4%
Within 1 day	1%
More than 1 day	0%
Cannot determine	10%
Total	100%

Q3. Does your company attempt to organize intelligence data based on perceived threat?	Pct%
Yes	43%
No	48%
Unsure	9%
Total	100%

Q4a. Did your company fail to stop a material security exploit because of insufficient or outdated cyber threat intelligence?	Pct%
Yes	60%
No	33%
Unsure	7%
Total	100%

Q4b. If yes, over the past 24 months, how many security exploits were not stopped because of insufficient or outdated cyber threat intelligence?	Pct%
None	23%
1 to 2	5%
3 to 4	8%
5 to 6	7%
7 to 8	9%
9 to 10	17%
More than 10	16%
Cannot determine	15%
Total	100%

Q5a. If your company's website, networks or enterprise systems were compromised, would you know it?	Pct%
Yes with certainty	10%
Yes, very likely	16%
Yes, likely	18%
Somewhat likely	19%
Unlikely	11%
No	26%
Total	100%

Q5b. If yes, on average, how long would take to know with a high degree of certainty that your company was compromised?	Pct%
Immediately	1%
Within 1 minute	3%
Within 1 hour	15%
Within 1 day	23%
Within 1 week	21%
Within 1 month	16%
More than 1 month	12%
Cannot determine	9%
Total	100%

Q6a. What enabling technologies does your company use to act on threat intelligence? Please select all that apply.	Pct%
SIEM	41%
Forensic tools	36%
Network intelligence	45%
URL content filtering	36%
Log and configuration management	43%
Intrusion detection systems	56%
Intrusion prevention systems	54%
Identity and authentication systems	65%
Whitelisting tools	27%
Blacklisting tools	31%
Endpoint security solutions	60%
Anti malware systems	88%
Anti denial of service (DDoS) systems	59%
Content aware firewalls	47%
Big data analytics	19%
Other (please specify)	0%
Average	44%

Q6b. Using the following 10-point scale, please rate the overall effectiveness of the above-mentioned technologies at providing you to with intelligence that reduces risk or mitigates attacks.	Pct%
1 or 2	16%
3 or 4	33%
5 or 6	29%
7 or 8	14%
9 or 10	8%
Total	100%

Q7a. Do you believe your company is presently targeted for attack?	Pct%
Yes with certainty	6%
Yes, very likely	21%
Yes, likely	20%
Somewhat likely	18%
Unlikely	11%
No	24%
Total	100%

Q7b. If yes, how do you know?	Pct%
Precise (dark) intelligence	23%
Logical deduction	12%
Warning from law enforcement	14%
CSCIRT	16%
Intuition (gut feel)	35%
Total	100%

Q8a. Where do you think an attack is most likely to come from [in the immediate future]? Please select two top choices.	Pct%
China (PRC)	67%
Southeast Asia plus ANZ	11%
Central and Northern Asia	3%
Russian Federation	54%
Eastern Europe	8%
Northern and Western Europe	3%
Middle East and Africa	19%
Latin America	4%
United States	24%
Don't know	5%
Other (please specify)	3%
Total	200%

Q8b. Where do you see the most attacks coming from [in the past and recent present]? Please select two top choices.	Pct%
China (PRC)	32%
Southeast Asia plus ANZ	6%
Central and Northern Asia	0%
Russian Federation	21%
Eastern Europe	11%
Northern and Western Europe	0%
Middle East and Africa	15%
Latin America	2%
United States	49%
Don't know	61%
Other (please specify)	3%
Total	200%

Q9. How certain are you about the geo-location (origin) of cyber attacks posed against your company?	Pct%
Very certain	13%
Certain	20%
Somewhat certain	23%
Not certain	44%
Total	100%

Q10. What types of cyber attacks against your company's networks cause the greatest concern? Please select the top three choices only.	Pct%
Cross-site scripting	5%
SQL and code injection	45%
Watering hole attacks	30%
Advanced persistent threats (APT)	57%
Login attacks	23%
Registration spamming	25%
Contact form or comment spam	19%
Root kits	54%
Clickjacking	37%
Other (please specify)	5%
Total	300%

Q11. What attacker presents the greatest cyber threat to your company today? Please select only one choice.	Pct%
Lone wolf hacker	9%
Malicious insider	21%
Criminal syndicates	34%
Hacktivists	17%
State sponsored attacker	19%
Other (please specify)	0%
Total	100%

Q12. In your opinion, how important is geo-location for determining the severity of cyber threats to your company?	Pct%
Essential	22%
Very important	31%
Important	19%
Not important	14%
Irrelevant	14%
Total	100%

Part 4. Live intelligence

Q13. In your opinion, how important is live intelligence to achieving a strong cyber security defense?	Pct%
Essential	30%
Very important	33%
Important	18%
Not important	11%
Irrelevant	8%
Total	100%

Q14a. Using the following 10-point effectiveness scale, please rate your company's ability to gather live cyber intelligence.	Pct%
1 or 2	40%
3 or 4	32%
5 or 6	15%
7 or 8	7%
9 or 10	6%
Total	100%

Q14b. Using the following 10-point effectiveness scale, please rate your company's ability to analyze and use actionable cyber intelligence.	Pct%
1 or 2	34%
3 or 4	31%
5 or 6	20%
7 or 8	8%
9 or 10	7%
Total	100%

Q15. In your opinion, how important is the use of big data analytics to achieving a strong cyber security defense?	Pct%
Essential	29%
Very important	30%
Important	16%
Not important	12%
Irrelevant	13%
Total	100%

Q16. What metrics do you (would you) use to assess the value of live intelligence? Please rank the following 6 choices from 1 = most important to 6 = least important.	Avg rank	Rank order
Increased ability to respond quickly to an existing cyber attack	1.88	1
Increased ability to prevent the exfiltration of confidential information	2.95	3
Increased ability to thwart future cyber attacks	2.16	2
Increased ability to prevent damages to IT infrastructure	4.91	5
Improved allocation of IT security resources	5.32	6
Reduced downtime of IT assets	3.89	4
Total	3.52	

Q17. Following are 9 features of enabling security solutions that attempt to generate actionable intelligence. Please rate each feature in terms of making the underlying reports more actionable and useful for companies using the following scale: 1=essential, 2 = very important, 3 = important, 4 = not important, 5 = irrelevant	Essential	Very important
Intelligence information is reported in ways that are not disruptive to IT operations or business processes	26%	32%
The communication and delivery of intelligence is based on a predetermined risk priority or level of the compromise	35%	35%
Intelligence reports are expedited once it is known that the company is targeted	31%	29%
The intelligence captures corroborating information from qualified external sources such as law enforcement, CSIRT and other third parties	19%	18%
The intelligence information includes trend data such as the velocity or frequency of attacks	28%	22%
Intelligence reports are clear, concise and unambiguous so that quick actions can be taken	35%	36%
Intelligence reports are automatically distributed to appropriate personnel based on their need to know	24%	23%
Intelligence information integrates with enabling technologies such as SIEM or other network monitoring tools	29%	37%

Part 5. Budget

Q18. Over the past 12 months, how much did cyber exploits cost your company? Please include all out-of-pocket expenses, productivity impact, legal costs and reputational damages.	Pct%
Zero costs	17%
Less than $500,000	6%
$500,000 to $1,000,000	7%
$1,000,001 to $5,000,000	20%
$5,000,001 to $10.000,000	28%
$10,000,001 to $25,000,000	12%
$25,00,001 to $50,000,000	7%
$50,00,001 to $100,000,000	1%
More than $100,000,000	2%
Total	100%

Q19. If your company could obtain actionable intelligence of cyber attacks within 60 seconds before compromise, how much less would these attacks cost your organization? Please express your estimate on a percentage to total cost as indicated above.	Pct%
No savings	15%
Less than 1%	3%
1% to 5%	2%
6% to 10%	7%
11% to 25%	16%
26% to 50%	18%
51% to 75%	18%
76% to 100%	21%
Total	100%

Q20. What determines how much your company spends on security in your IT budget? Please select only one top reason.	Pct%
The frequency of attacks experienced	29%
The severity of attacks experienced	26%
Attacks on companies in your industry	6%
Media stories and news headlines	5%
Legal and compliance requirements	31%
Reputation preservation	3%
Other (please specify)	0%
Total	100%

Q21a. Approximately, what best describes your company's IT spending in the present year? Please include all direct and indirect costs including technology investments, labor costs and overhead.	Pct%
Less than $1,000,000	4%
$1,000,000 to $5,000,000	2%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	11%
$25,000,001 to $50,000,000	30%
$50,00,001 to $100,000,000	31%
$100,000,001 to $500,000,000	10%
More than $500,000,000	5%
Total	100%

Q21b. Approximately, what percentage of the above IT spending level is dedicated to IT security?	Pct%
Less than 1%	0%
1 to 5%	4%
6 to 10%	27%
11 to 15%	33%
16 to 20%	21%
21 to 25%	11%
26 to 30%	3%
31 to 35%	0%
36 to 40%	1%
41 to 45%	0%
46 to 50%	0%
More than 50%	0%
Total	100%

Q21c. Approximately, what percentage of the above IT security budget is earmarked for systems or processes that produce intelligence about cyber threats?	Pct%
Less than 1%	11%
1 to 5%	2%
6 to 10%	4%
11 to 15%	14%
16 to 20%	22%
21 to 25%	18%
26 to 30%	14%
31 to 35%	10%
36 to 40%	3%
41 to 45%	1%
46 to 50%	1%
More than 50%	0%
Total	100%

Q21d. Twelve (12) months from now, what will be the percentage of the IT security budget earmarked for systems or processes that produce intelligence about cyber threats?.	Pct%
Less than 1%	8%
1 to 5%	1%
6 to 10%	3%
11 to 15%	7%
16 to 20%	13%
21 to 25%	15%
26 to 30%	23%
31 to 35%	12%
36 to 40%	12%
41 to 45%	4%
46 to 50%	1%
More than 50%	1%
Total	100%

Part 6. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Executive/VP	3%
Director	16%
Manager	21%
Supervisor	18%
Technician	35%
Staff	6%
Contractor/Consultant	1%
Other	0%
Total	100%

D2. Check the Primary Person you or your immediate supervisor reports to within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer	0%
General Counsel	0%
Chief Information Officer	60%
Chief Technology Officer	4%
Chief Information Security Officer	20%
Compliance Officer	6%
Chief Privacy Officer	0%
Human Resources VP	0%
Chief Security Officer	2%
Chief Risk Officer	7%
Other (please specify)	0%
Total	100%

D3. Total years of relevant experience	Mean	Median
Total years of IT or security experience	11.07	10.50
Total years in current position	6.27	6.00

D4. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	6%
Defense	1%
Education & research	2%
Energy & utilities	3%
Entertainment & media	2%
Financial services	19%
Health & pharmaceutical	12%
Hospitality	4%
Industrial	6%
Public sector	12%
Retail	9%
Services	9%
Technology & software	6%
Transportation	2%
Other	3%
Total	100%
D5. Where are your employees located? (Check all that apply):	**Pct%**
United States	100%
Canada	69%
Europe	67%
Middle East & Africa	53%
Asia-Pacific	59%
Latin America (including Mexico)	51%
All economic regions	48%
D6. What is the worldwide headcount of your organization?	**Pct%**
Less than 500	12%
500 to 1,000	27%
1,001 to 5,000	31%
5,001 to 25,000	19%
25,001 to 75,000	6%
More than 75,000	5%
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.

About Norse

Norse is the leading innovator in the live threat intelligence security market. With the goal of transforming the traditionally reactive IT security industry, Norse offers proactive, intelligence-based security solutions that enable organizations to identify and defend against the advanced cyber threats of today and tomorrow. Norse's synchronous, global platform is a patent-pending infrastructure-based technology that continuously collects and analyzes real-time, high risk Internet traffic to identify the sources of cyber attacks and fraud. Norse is the only provider of live, actionable, cyber threat intelligence that enables organizations to prevent financial fraud and proactively defend against today's most advanced cyber threats including zero day and advanced persistent threats. Norse has offices in Silicon Valley, St. Louis, and Atlanta. Visit us online at norse-corp.com.

Norse Sales and Support inquiry@norse-corp.com