Tone at the Top and Third Party Risk

Sponsored by Shared Assessments

Independently conducted by Ponemon Institute LLC

Publication Date: May 2016

Tone at the Top and Third Party Risk

Ponemon Institute and Shared Assessments: May 2016

Part 1. Introduction

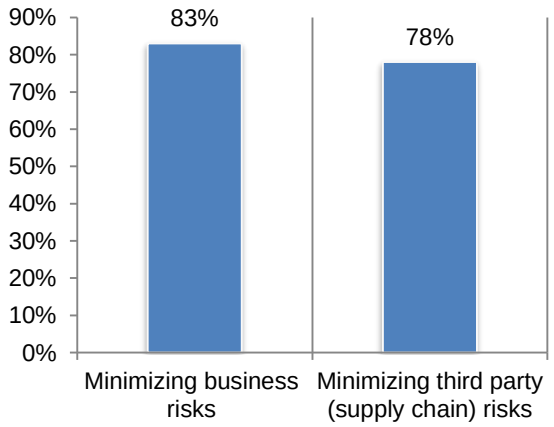
Tone at the Top and Third Party Risk was sponsored by Shared Assessments and conducted by Ponemon Institute to understand the relationship between tone at the top and the minimization of third party risks. We surveyed 617 individuals who have a role in the risk management process in their organizations and are familiar with the governance practices related to third party risks.

A key takeaway from the research is that accountability for managing third party risk is dispersed throughout the organization. Not having one person or function with ownership of the risk is a serious barrier to achieving an effective third party risk management program.

In the context of this study, tone at the top is a term used to describe an organization's control environment, as established by its board of directors, audit committee and senior management. The tone at the top is set by all levels of management and has a trickle-down effect on all employees of the organization. If management is committed to a culture and environment that embraces honesty, integrity and ethics, employees are more likely to uphold those same values. As a result, such risks as insider negligence and third party risk are minimized.

Participants in this research agree with this assessment. We asked respondents to rate the importance of tone at the top based on a scale of 1 = not important to 10 = very important. The very important responses (7+) are shown in Figure 1. As shown, 83 percent of respondents believe a positive tone is very important to minimizing business risks within their organization and 78 percent of respondents say it is very important to reducing risks in third party (supply chain) relationships.

Figure 1. How important is a positive tone at the top to minimizing business and third party risk?
1 = not important to 10 = very important, 7 + responses



A positive tone at the top is thought to provide the following benefits, according to respondents:

- Reduces the risks of working with third parties that are not trustworthy (71 percent of respondents);
- Incorporates such values as integrity, ethics and trustworthiness in relationships with third parties (66 percent of respondents); and
- Increases employee and third party awareness of the importance of security, data protection and business resiliency (43 percent of respondents).

The following are key takeaways from the research:

The state of third party risk management

- **Third party risk is considered serious and is increasing.** Seventy-five percent of respondents agree that third party risk is serious. Further, 70 percent of respondents say the

third party risk in their organization is significantly increasing (21 percent of respondents), increasing (20 percent of respondents) or is staying the same (29 percent of respondents).

- **Third party risk is increasing because of a changing threat landscape**. Disruptive technologies such as the Internet of Things (IoT) and migration to the Cloud are expected to increase third party risk. Sixty percent of respondents believe IoT increases third party risk significantly (35 percent + 25 percent), and 68 percent of respondents believe migration to the Cloud will increase risk (36 percent + 32 percent).

- **Cyber attacks and the IoT are expected to have the most significant impact on an organization's third party risk profile**. Seventy-eight percent of respondents say cyber attacks will have a significant impact on the risk profile and 76 percent of respondents say the IoT will have a significant impact. Cloud computing, mobility and mobile devices and big data analytics will have a significant impact, according to 71 percent, 67 percent and 51 percent of respondents, respectively.

- **Despite the seriousness of third party risk, it is not a primary risk management objective.** The top two risk management objectives are to minimize downtime (56 percent of respondents) and minimize business disruptions (37 percent of respondents). As discussed above, cyber attacks are expected to have a significant impact on the risk of third party relationships. However, only 27 percent of respondents say a top objective is to prevent cyber attacks. Further, only 8 percent of respondents say improvement of their organization's relationship with business partners is a top risk management objective for their organizations.

- **The consequences of not managing third party risk can be costly.** In the past 12 months, organizations represented in this research spent an average of approximately $10 million to respond to a security incident as a result of negligent or malicious third parties.

- **Third party risk management programs are mostly informal and not effective.** As discussed previously, reducing third party risk is considered serious but very few respondents say improvement in third party relationships is a top risk management objective. Thus, the incentive among the various business functions to create a comprehensive program for risk management is low. Only 29 percent of respondents say their organizations have a formal program.

- **The lack of formal programs affects the ability to mitigate third party risk.** Respondents were asked to rate the effectiveness of their organizations in mitigating or curtailing third party risk from 1 = not effective to 10 = very effective. Only 21 percent of respondents say their organization's effectiveness in mitigating or curtailing third party risk is considered highly effective (7+ on the scale of 1 to 10).

- **No one function owns the third party risk management program in organizations represented in this study**. Accountability for the third party risk management program is dispersed throughout the organization. Twenty-three percent of respondents say the compliance department is most responsible for managing third party risk and 17 percent of respondents say it is the information security function. Only 9 percent of respondents say risk management has ownership of the risk.

- **Most C-level executives are not engaged in their organization's third party risk management process.** Only 37 percent of respondents agree that the C-level executives in their organization believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management.

- **Boards of directors are not actively engaged in risk management activities.** Similar to the perceived lack of accountability on the part of C-suite executives, only 40 percent of respondents say their boards of directors are significantly involved (17 percent) or have at least some involvement in overseeing risk management activities (23 percent).

- **If boards of directors are engaged, it is mostly to conduct reviews.** Fifty-two percent of respondents say the board mainly reviews management's analysis of the effectiveness of a risk assessment and 42 percent of respondents say the board reviews and approves plans to address any risk management or control weakness. Only 25 percent of respondents say they are actively working with management to establish the vision, risk appetite and overall strategic direction for third party relationships.

The importance of values and a positive tone to effective third party risk management

- **Organizations in this study are not effective in communicating their values.** Only 11 percent of respondents say their organizations are very effective at communicating values throughout the enterprise or to business partners, vendors and other third parties. Sixteen percent of respondents say values are not communicated throughout the enterprise and 15 percent say values are not communicated to business partners, vendors and other third parties.

- **The CEO is expected to set a positive tone.** Forty-one percent of respondents say it should be the CEO who sets the tone at the top, followed by 19 percent of respondent who say it is the compliance officer. Only 6 percent of respondents say the C-suite is most responsible for setting a positive tone at the top for the entire organization.

- **Trustworthiness of third parties is the most important benefit of a positive tone at the top.** Seventy-one percent of respondents say that when tone at the top is part of an organization's risk management strategy the risk of working with third parties that are not trustworthy is reduced. Sixty-six percent of respondents say their organizations incorporate such values as integrity, ethics and trustworthiness in relationships with third parties.

- **To communicate values to employees and other stakeholders, organizations rely upon codes of conduct and mentoring.** Sixty-five percent of respondents say their organizations use a code of conduct to communicate values throughout the organization, and 53 percent of respondents say on the job mentoring is how values are communicated. Training and policies, which would ensure a more comprehensive and consistent communication of values, are not used as often (50 percent and 41 percent of respondents, respectively).

- **Organizations are almost evenly divided on whether to ensure there is no retaliation when reporting unethical behavior**. Fifty-six percent of respondents say their organization provides a path for employees who are witnessing unethical behavior to be able to report such behavior without fear of retaliation and guaranteed anonymity, and 53 percent of respondents say their organization would not retaliate against business partners, vendors and other third parties who report unethical behavior.

Third party risk assessment and management practices

- **The process to assess third party risk is ineffective.** Only 26 percent of respondents say their assessment of controls of business partners, vendors and third parties is effective. In fact, 30 percent of respondents say their organizations do not assess these controls. If they do assess controls, the most common practice is to do a legal review (55 percent of respondents) or through required contract clauses (plus indemnification) (47 percent of respondents). As discussed, 44 percent of respondents say their organizations conduct a risk based assessment. Most of the respondents say it is an informal process that is customized

for different types of third party relationships (30 percent of respondents) or the assessment is ad hoc (29 percent of respondents).

- **The compliance function, not risk management, is most responsible for risk assessment processes.** In those organizations that conduct risk assessments to evaluate the controls of business partners, vendors and other third parties, the compliance function is likely to both execute and take responsibility to ensure that the risk assessment is completed and all risks are addressed, according to 23 percent and 32 percent of respondents, respectively. Following compliance, the lines of business are the second most likely function to make sure assessments are completed and risks assessed, according to 27 percent of respondents. Very often the lines of business are the first line of defense in protecting sensitive and confidential information in the hands of third parties.

- **If the assessment revealed a lack of controls, would the organization cease or terminate an agreement?** One-third of respondents say it would be unlikely that their organization would cease or terminate an agreement with a third party that is unable to meet their control requirements. However, more respondents (43 percent of respondents) say that it is very likely or likely the third party would be fired.

- **Why is third party risk assessment failing in organizations?** The following three factors contribute to the ineffectiveness of third party risk assessments:

  First, 56 percent of respondents say the risk assessment does not reveal the intellectual property (IP) and other high value data that are in the hands of third parties.

  Second, only 31 percent of respondents say they have metrics to measure the effectiveness of risk management activities. As a result, very few organizations in this research are considered to have a highly effective risk management process—probably because they are not attempting to measure its effectiveness.

  Third, only 18 percent of respondents say they assess the cyber security risks of most third parties. Almost half (49 percent of respondents) say they do not conduct such assessments.

The use of technologies and cyber insurance to manage third party risks

- **What top technologies do organizations require their third parties to have in place?** The top three technologies and practices third parties are expected to have are: anti-virus/anti-malware, intrusion detection and prevention systems and identity management and authentication.

- **Companies are not procuring cyber insurance to reduce third party risks.** While organizations may be purchasing cyber insurance to reduce their own risks, only 26 percent of respondents say they are procuring such insurance to reduce the economic impact of third party risk. However, 43 percent of respondents do require most (17 percent of respondents) or some (26 percent of respondents) business partners, vendors and other third parties to buy such insurance. Lines of business (20 percent of respondents) and the legal department (19 percent of respondents) are most responsible for verifying that the cyber insurance coverage is sufficient for the risk associated with the services received.

Part 2. Key findings

In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of this report.

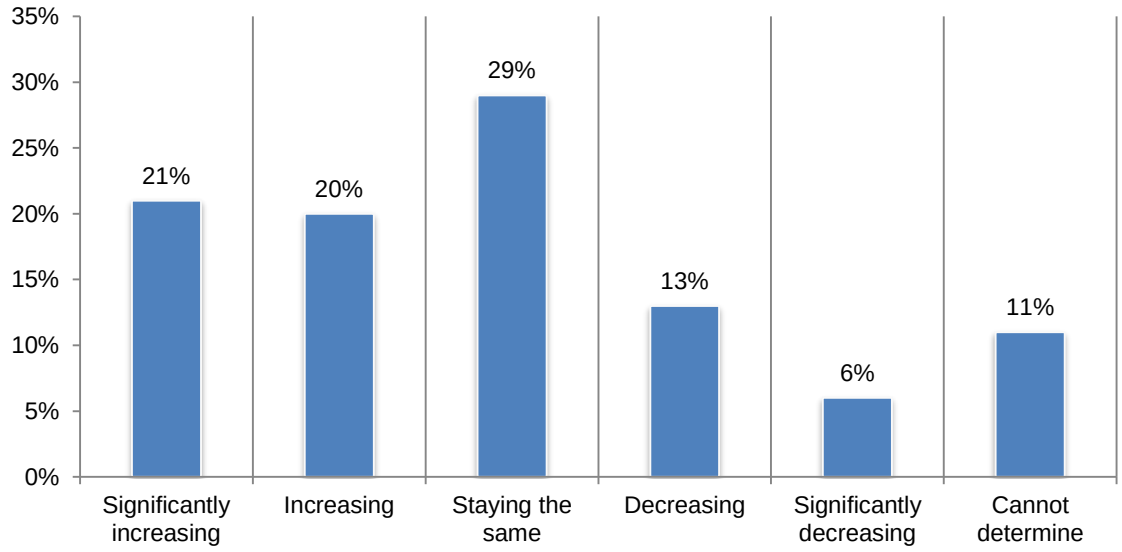
We have organized the findings in this research according to the following topics:

- The state of third party risk management;
- The importance of values and a positive tone to effective third party risk management;
- Third party risk assessment and management practices;
- The use of technologies and cyber insurance to manage third party risk; and
- Conclusion: Ten steps to creating a stronger third party risk management program.

The state of third party risk management

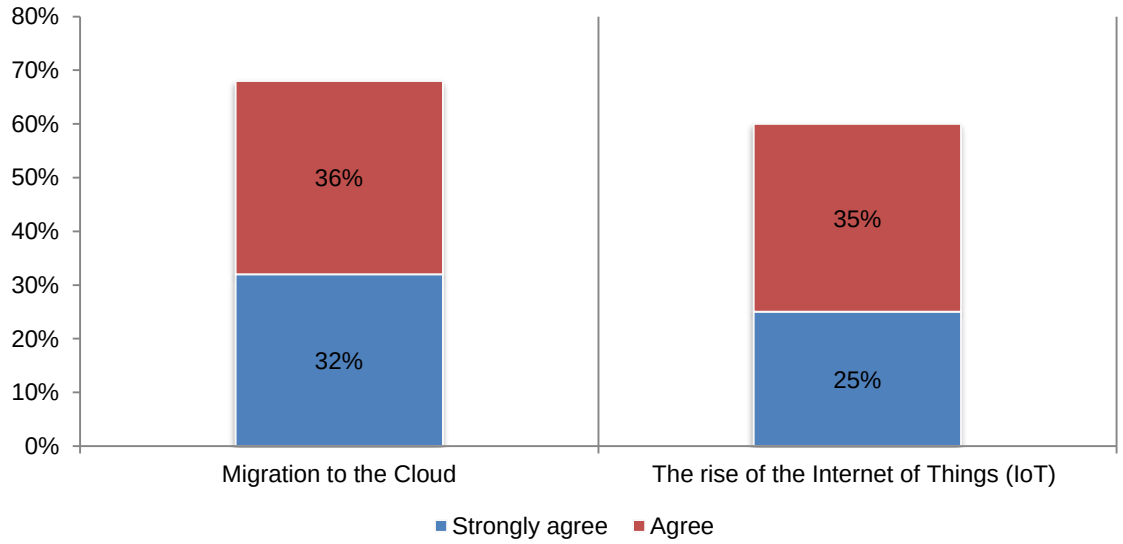
Third party risk is considered serious and is increasing. Seventy-five percent of respondents agree that third party risk is serious. Further, as shown in Figure 2, 70 percent of respondents say the third party risk in their organization is significantly increasing (21 percent of respondents), increasing (20 percent of respondents) or is staying the same (29 percent of respondents).

Figure 2. Is third party risk increasing, decreasing or staying the same?



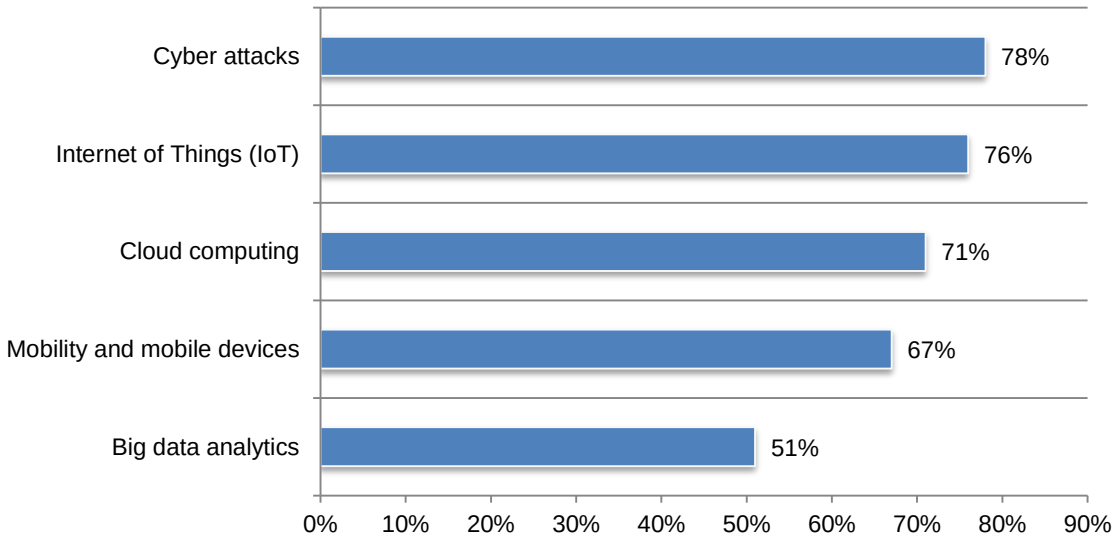
Third party risk is increasing because of a changing threat landscape. Disruptive technologies such as the IoT and migration to the Cloud are expected to increase third party risk. As shown in Figure 3, 60 percent of respondents believe the IoT increases third party risk significantly (35 percent + 25 percent) and 68 percent of respondents believe migration to the Cloud will increase risk (36 percent + 32 percent).

Figure 3. IoT and migration to the Cloud will increase third party risk.
Strongly agree and agree responses combined



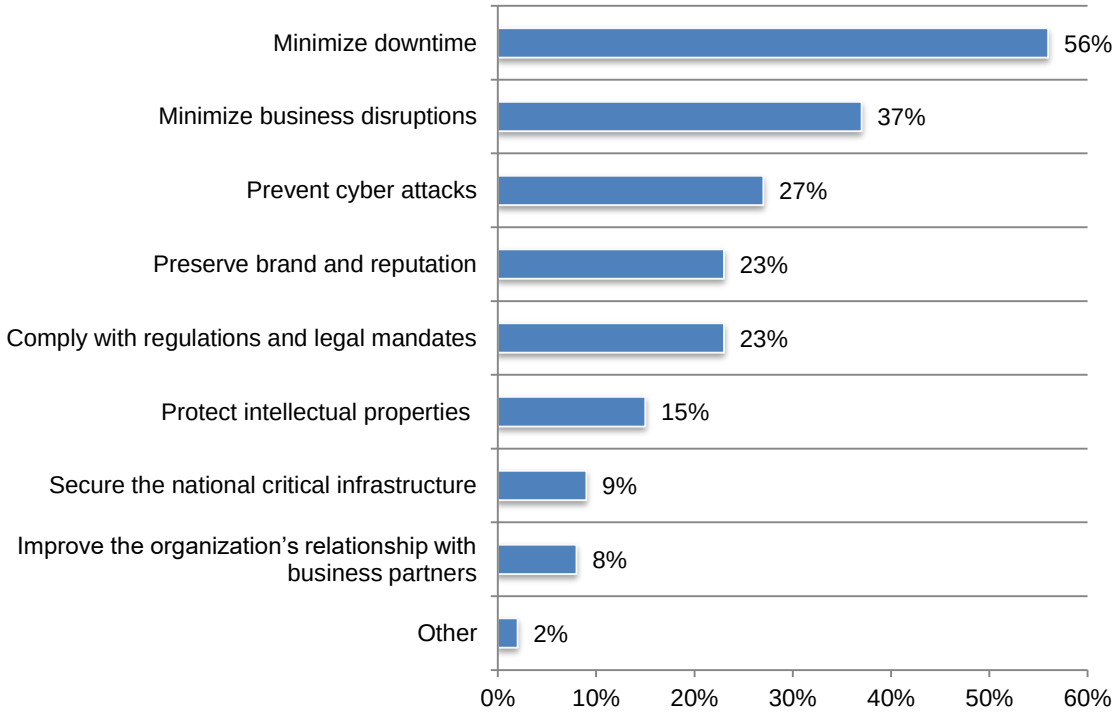
Cyber attacks and the IoT are expected to have the most significant impact on an organization's third party risk profile. According to Figure 4, 78 percent of respondents say cyber attacks will have a significant impact on the risk profile and 76 percent of respondents say the IoT will have a significant impact. Cloud computing, mobility and mobile devices and big data analytics will have a significant impact, according to 71 percent, 67 percent and 51 percent of respondents, respectively.

Figure 4. What trends will have a significant impact on an organization's third party risk?
7+ responses on a scale from 1 = no impact to 10 = significant impact



Despite the seriousness of third party risk, it is not a primary risk management objective. According to Figure 5, the top two risk management objectives are to minimize downtime (56 percent of respondents) and minimize business disruptions (37 percent of respondents). As discussed above, cyber attacks are expected to have a significant impact on the risk of third party relationships. However, only 27 percent of respondents say that a top objective is to prevent cyber attacks. Further, only 8 percent of respondents say improvement of their organization's relationship with business partners is a top risk management objective for their organizations.

Figure 5. What are the top two risk management objectives within your organization?
Two choices were permitted

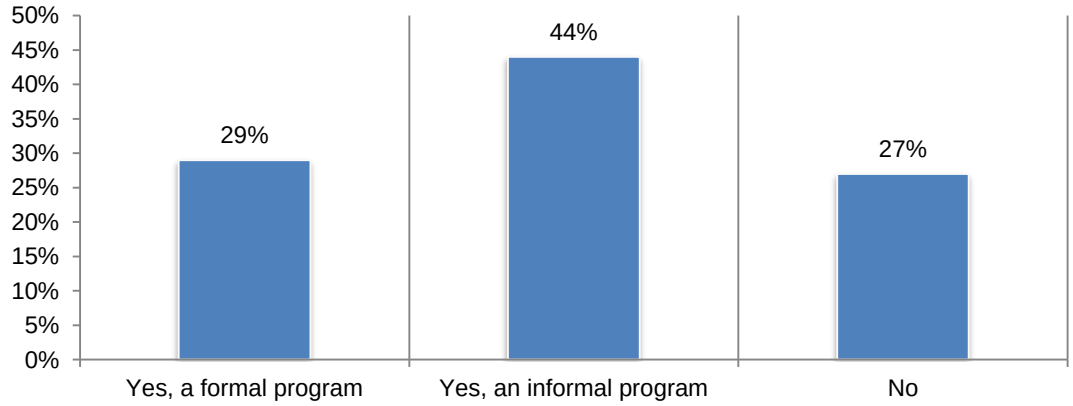


The consequences from not managing third party risk can be costly. In the past 12 months, organizations represented in this research spent an average of approximately $10 million to respond to a security incident as a result of negligent or malicious third parties. These costs include the direct cash outlay for the following activities:

- Remediation and technical support activities including forensic investigations, incident response activities, help desk and customer service operations;
- Users' idle time and lost productivity because of downtime or system performance delays;
- Disruption to normal operations because of system availability problems;
- Damage or theft of assets and infrastructure; and
- Reputation loss and brand damages.

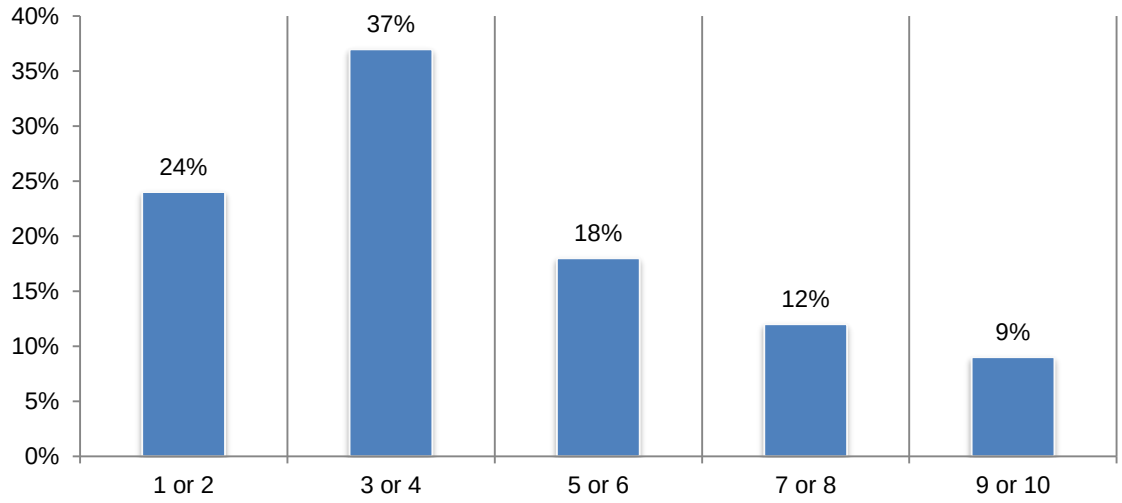
Third party risk management programs are mostly informal and not effective. As discussed previously, reducing third party risk is considered serious but very few respondents say improvement in third party relationships is a top risk management objective. Thus, the incentive among the various business functions to create a comprehensive program for risk management is low. As shown in Figure 6, only 29 percent of respondents say their organizations have a formal program.

Figure 6. Does your organization have a program for managing third party risks?



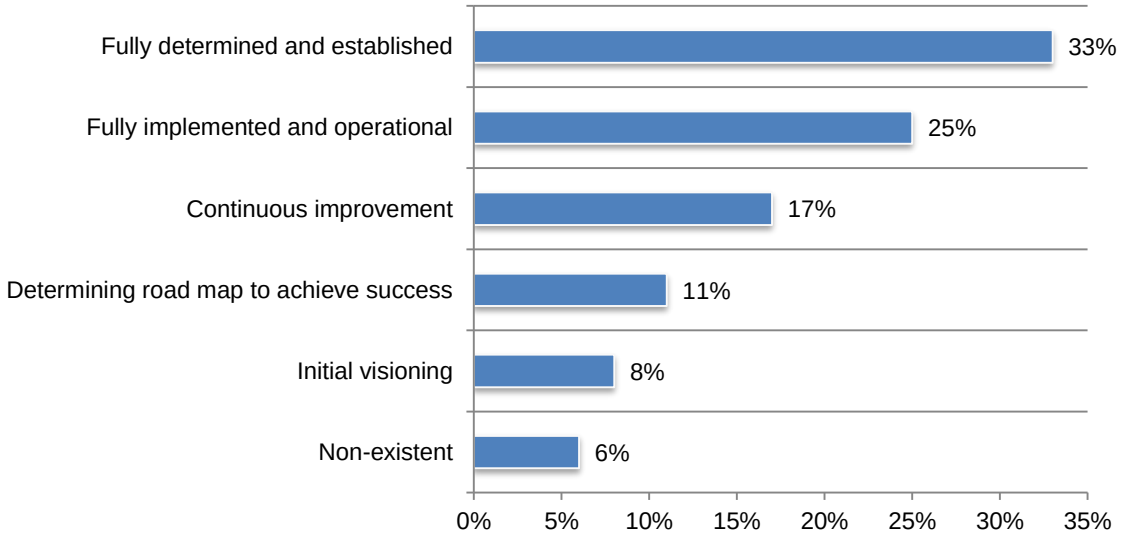
The lack of formal programs affects the ability to mitigate third party risk. Respondents were asked to rate the effectiveness of their organizations in mitigating or curtailing third party risk from 1 = not effective to 10 = very effective. As shown in Figure 7, only 21 percent of respondents say their organization's effectiveness in mitigating or curtailing third party risk is considered highly effective (7+ on the scale of 1 to 10).

Figure 7. How effective is your organization in mitigating or curtailing third party risk?
1 = not effective to 10 = very effective



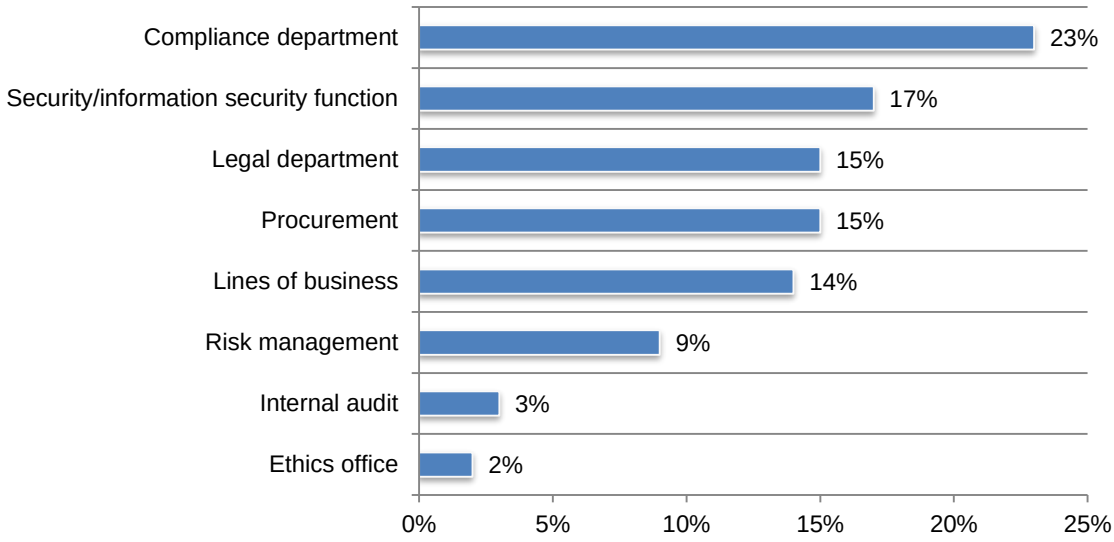
These respondents say the maturity level of their organization's risk management program or activities are fully determined and established (33 percent of respondents), fully implemented and operational (25 percent of respondents) or in a state of continuous improvement (17 percent of respondents), according to Figure 8.

Figure 8. What best describes the maturity level of your organization's risk management program or activities?



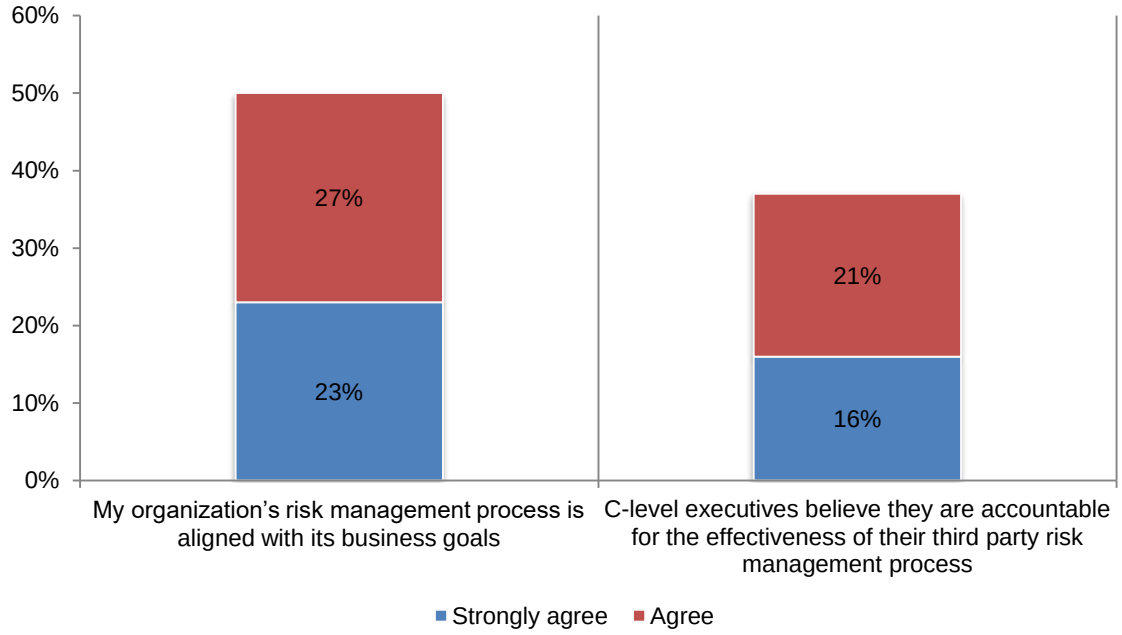
No one function owns the third party risk management program in organizations represented in this study. Accountability for the third party risk management program is dispersed throughout the organization. As shown in Figure 9, 23 percent of respondents say the compliance department is most responsible for managing third party risk and 17 percent of respondents say it is the information security function. Only 9 percent of respondents say ownership is assigned to risk management.

Figure 9. Which department is most likely to own third party risk management in your organization?



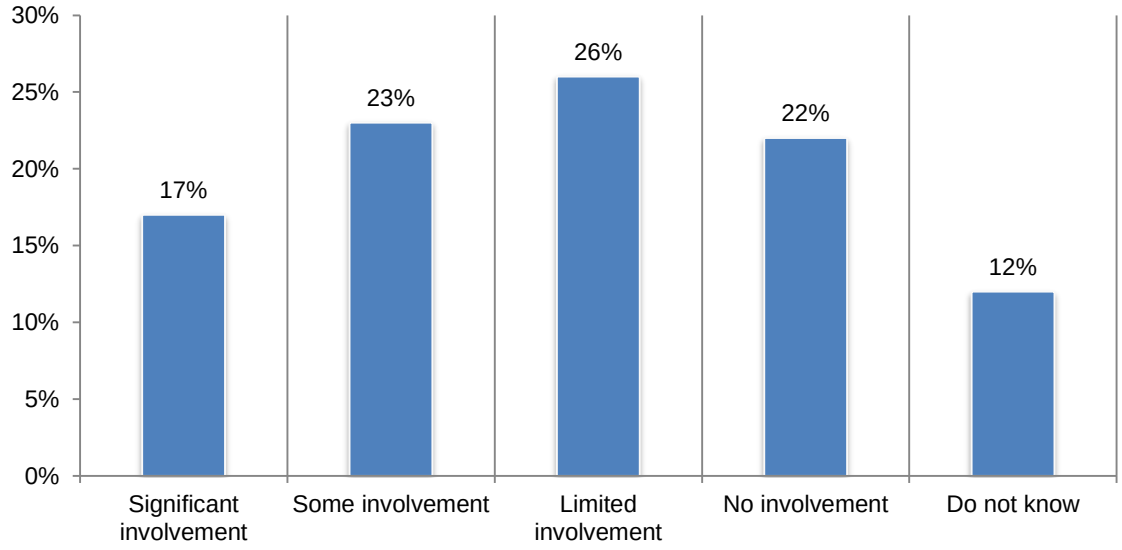
Most C-level executives are not engaged in their organization's third party risk management process. According to Figure 10**,** only 37 percent of respondents agree that the C-level executives in their organization believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management.

Figure 10. Perceptions about the third party risk management process.



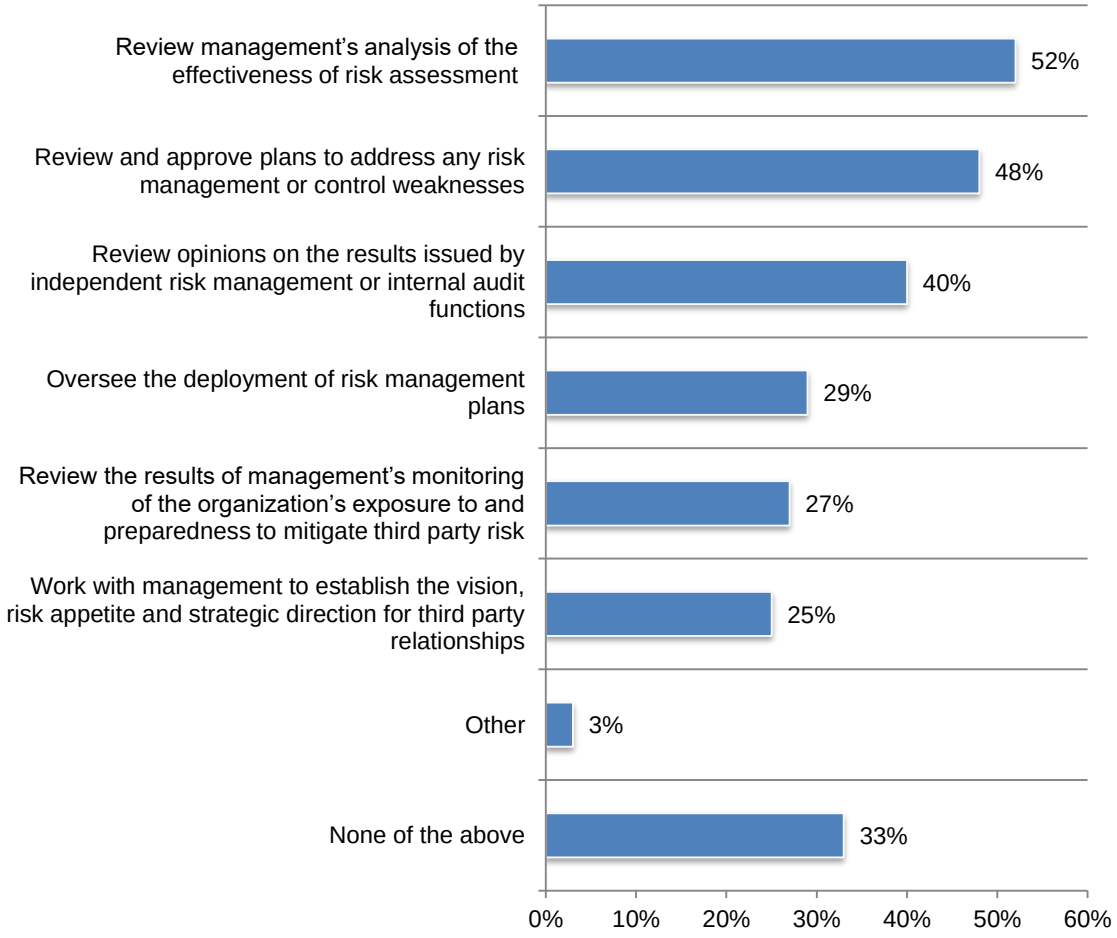
Boards of directors are not actively engaged in risk management activities. Similar to the perceived lack of accountability on the part of C-suite executives, only 40 percent of respondents say their boards of directors are significantly involved (17 percent) or have at least some involvement in overseeing risk management activities (23 percent), as shown in Figure 11.

Figure 11. How involved is the board of directors in overseeing risk management activities?



If boards of directors are engaged, it is mostly to conduct reviews. According to Figure 12, 52 percent of respondents say the board mainly reviews management's analysis of the effectiveness of a risk assessment and 42 percent of respondents say the board reviews and approves plans to address any risk management or control weakness. Only 25 percent of respondents say they are actively working with management to establish the vision, risk appetite and overall strategic direction for third party relationships.

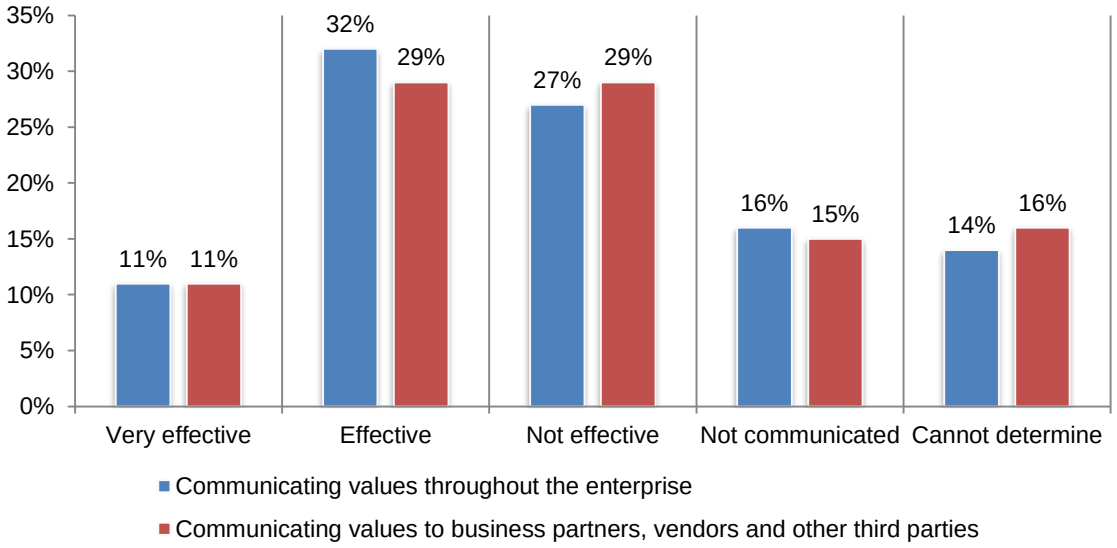
Figure 12. What activities are the boards of directors involved in?



The importance of values and a positive tone to effective third party risk management

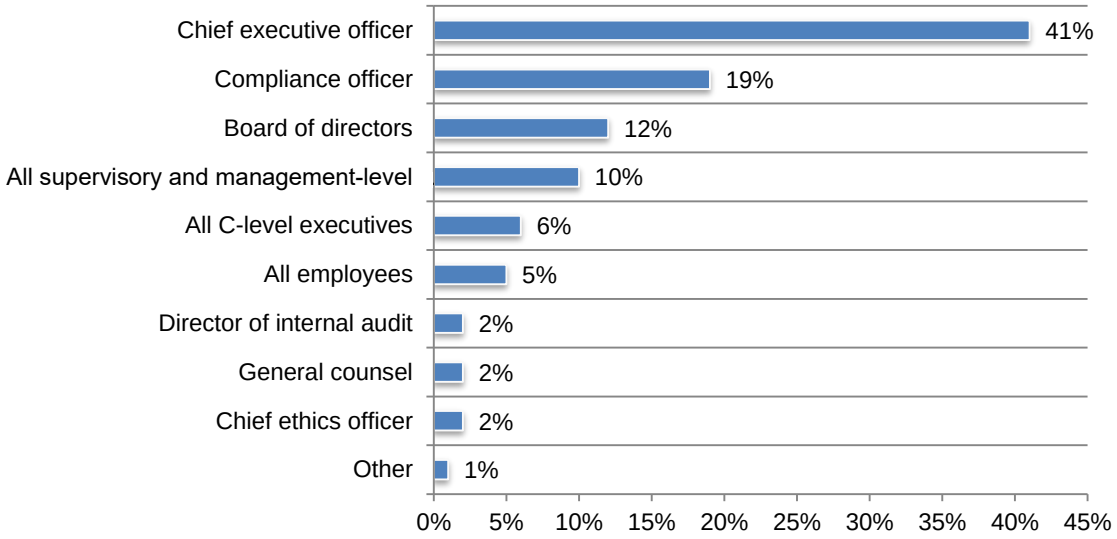
Organizations in this study are not effective in communicating their values. Only 11 percent of respondents say their organizations are very effective at communicating values throughout the enterprise or to business partners, vendors and other third parties, as shown in Figure 13. Sixteen percent of respondents say values are not communicated throughout the enterprise and 15 percent say values are not communicated to business partners, vendors and other third parties.

Figure 13. How effective is your organization at communicating values throughout the enterprise and to third parties?



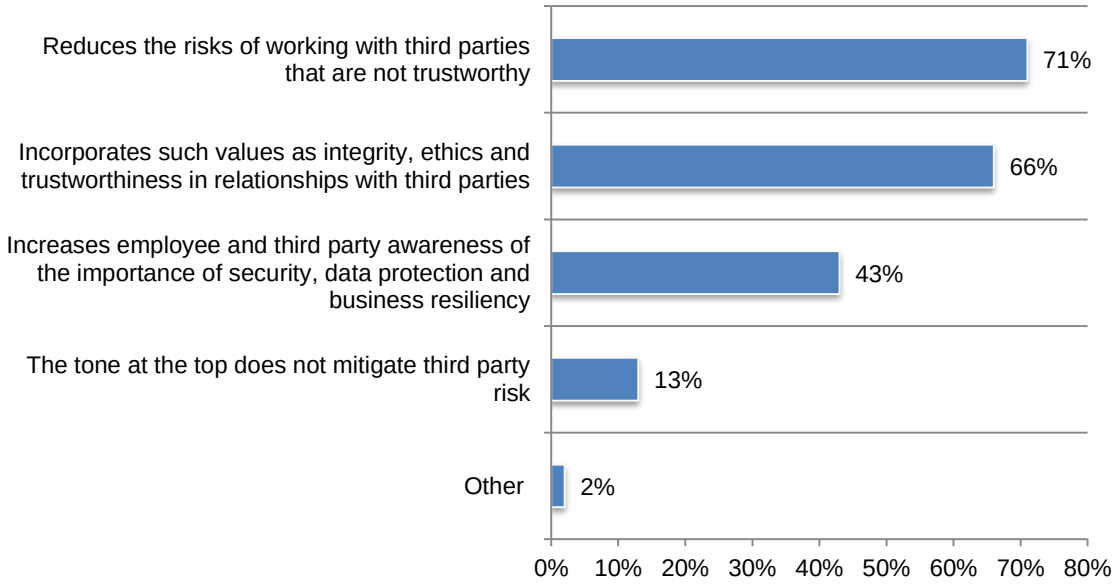
The chief executive officer is expected to set a positive tone. According to Figure 14, 41 percent of respondents say it should be the chief executive director who sets the tone at the top, followed by 19 percent of respondent who say it is the compliance officer. Only 6 percent of respondents say the C-suite is most responsible for setting a positive tone at the top for the entire organization.

Figure 14. Who is most responsible for setting a positive tone for your organization?



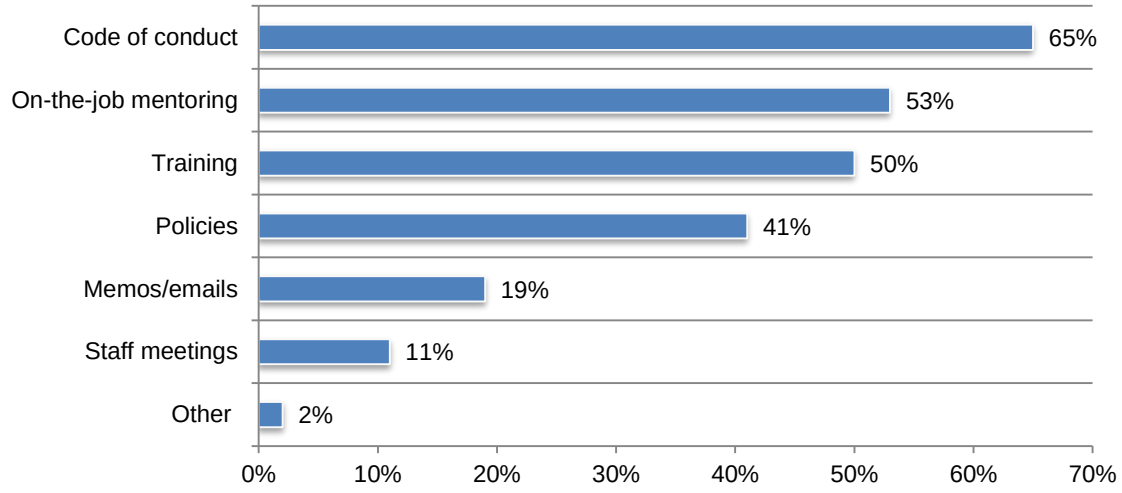
Trustworthiness of third parties is the most important benefit of a positive tone at the top. As shown in Figure 15**,** 71 percent of respondents say that when tone at the top is part of an organization's risk management strategy, the risk of working with third parties that are not trustworthy is reduced. Sixty-six percent of respondents say their organizations incorporate such values as integrity, ethics and trustworthiness in relationships with third parties.

Figure 15. How does the tone at the top mitigate third party risk?
More than one choice was permitted



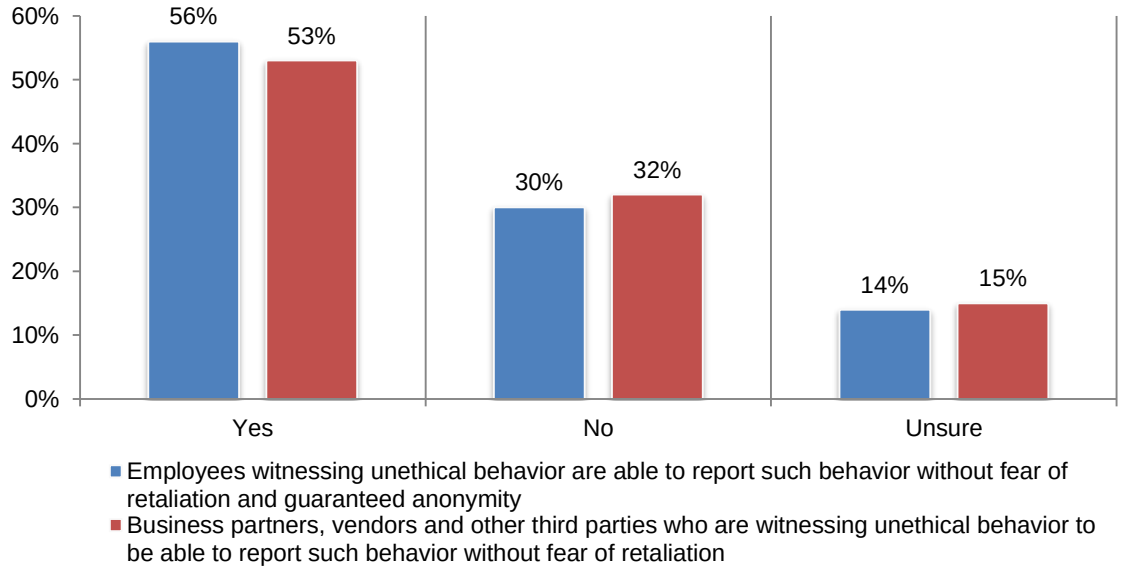
To communicate values to employees and other stakeholders, organizations rely upon codes of conduct and mentoring. Sixty-five percent of respondents say their organizations use a code of conduct to communicate values throughout the organization and 53 percent of respondents say on the job mentoring is how values are communicated, as shown in Figure 16. Training and policies, which would ensure a more comprehensive and consistent communication of values, are not used as often (50 percent and 41 percent of respondents, respectively).

Figure 16. How does your organization communicate its values to employees and other stakeholders?
More than one choice was permitted



Organizations are almost evenly divided on whether to ensure there is no retaliation when reporting unethical behavior. According to Figure 17, 56 percent of respondents say their organization provides a path for employees who are witnessing unethical behavior to be able to report such behavior without fear of retaliation and guaranteed anonymity, and 53 percent of respondents say their organization would not retaliate against business partners, vendors and other third parties who report unethical behavior.

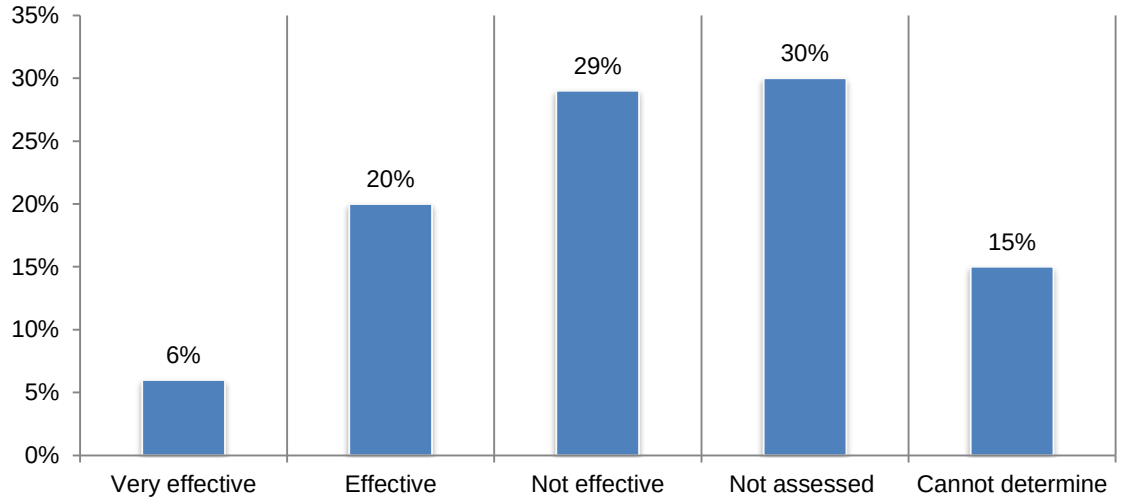
Figure 17. Does your organization provide a way for employees and third parties to report unethical behavior without retaliation?



Third party risk assessment and management practices

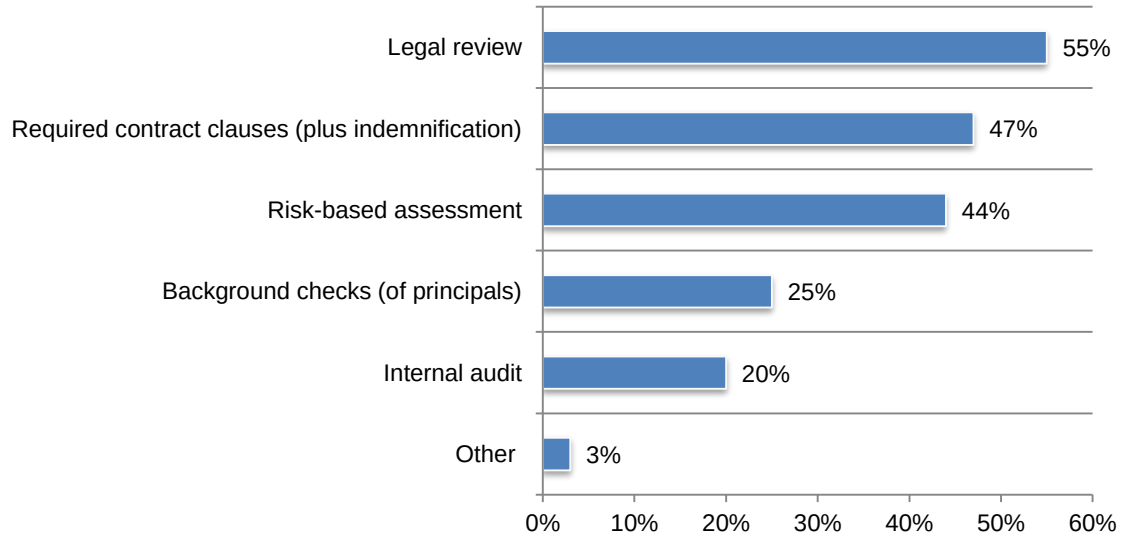
The process to assess third party risk is ineffective. Only 26 percent of respondents say their assessment of controls of business partners, vendors and third parties is effective. In fact, 30 percent of respondents say their organizations do not assess these controls, as shown in Figure 18.

Figure 18. How effective is your organization at assessing third party controls to reduce risks?



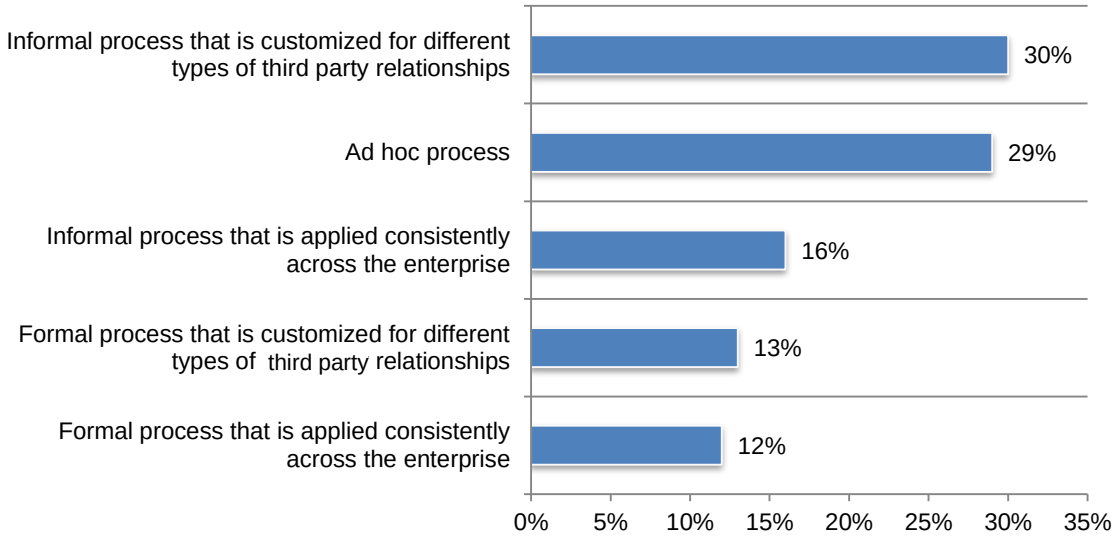
If organizations do assess controls, the most common practice is to do a legal review (55 percent of respondents) or through required contract clauses (plus indemnification) (47 percent of respondents), according to Figure 19.

Figure 19. How are third party controls to reduce risks assessed?
More than one choice permitted



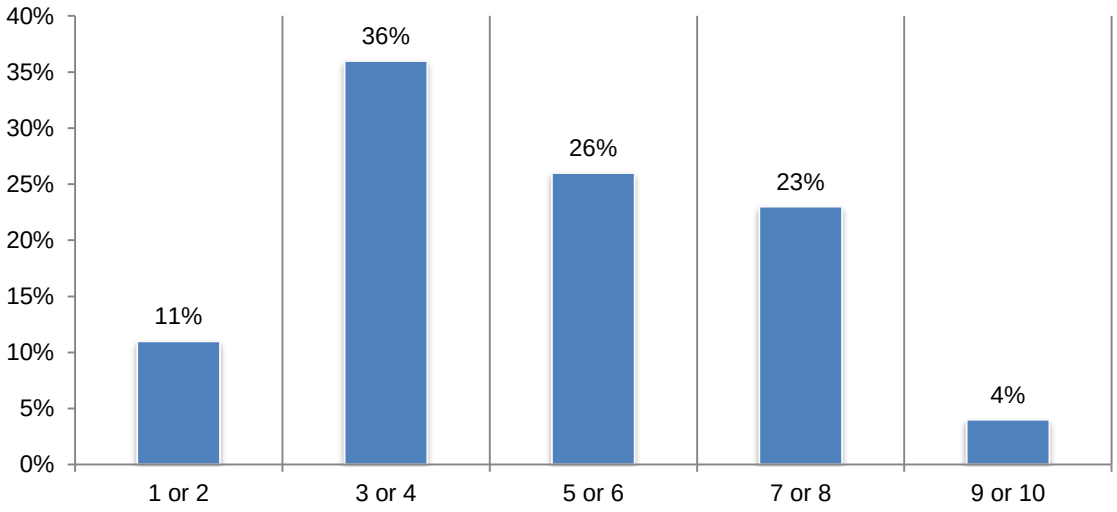
As shown above, 44 percent of respondents say their organizations conduct a risk-based assessment. Figure 20 reports the risk assessment process in these organizations. Most of the respondents say it is an informal process that is customized for different types of third party relationships (30 percent of respondents) or the assessment is ad hoc (29 percent of respondents).

Figure 20. What best describes the risk assessment process?



However, only 27 percent of these respondents rate the effectiveness of risk assessments at determining the control environment of business partners, vendors and other third parties as very effective, as shown in Figure 21.

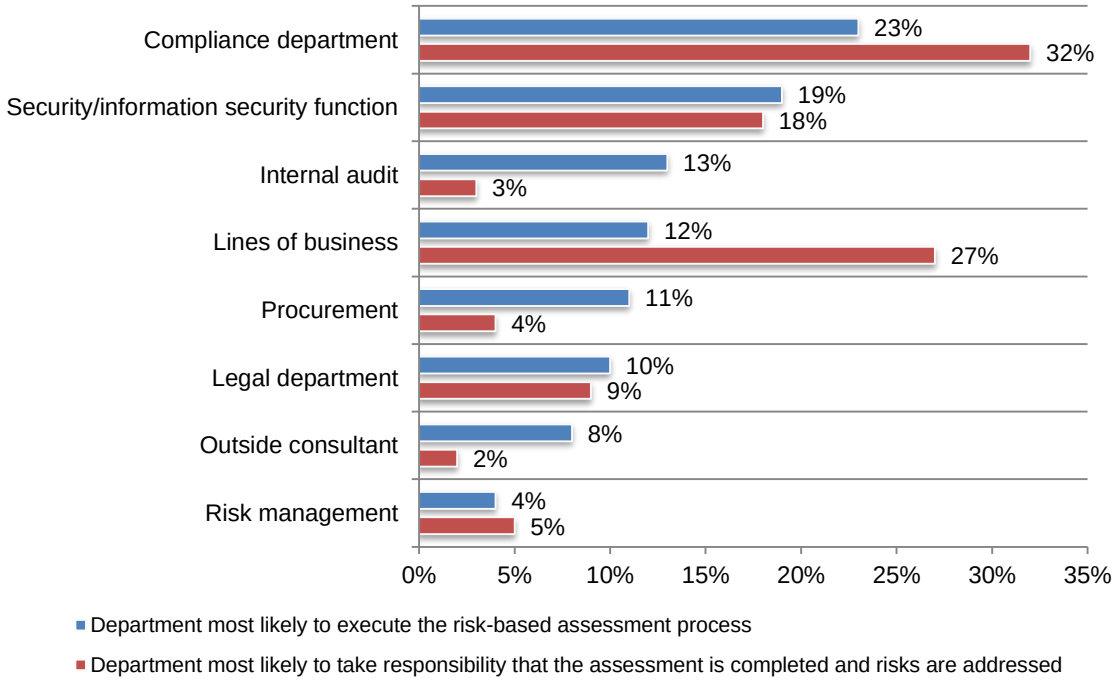
Figure 21. How effective are risk assessments at determining the control environment of third parties?



The compliance function, not risk management, is most responsible for risk assessment processes. In those organizations that conduct risk assessments to evaluate the controls of business partners, vendors and other third parties, the compliance function is likely to both execute and take responsibility to ensure that the risk assessment is completed and all risks are addressed, according to 23 percent and 32 percent of respondents, respectively (Figure 22).

Following compliance, the lines of business are the second most likely function to make sure assessments are completed and risks assessed, according to 27 percent of respondents. Very often the lines of business are the first line of defense in protecting sensitive and confidential information in the hands of third parties.

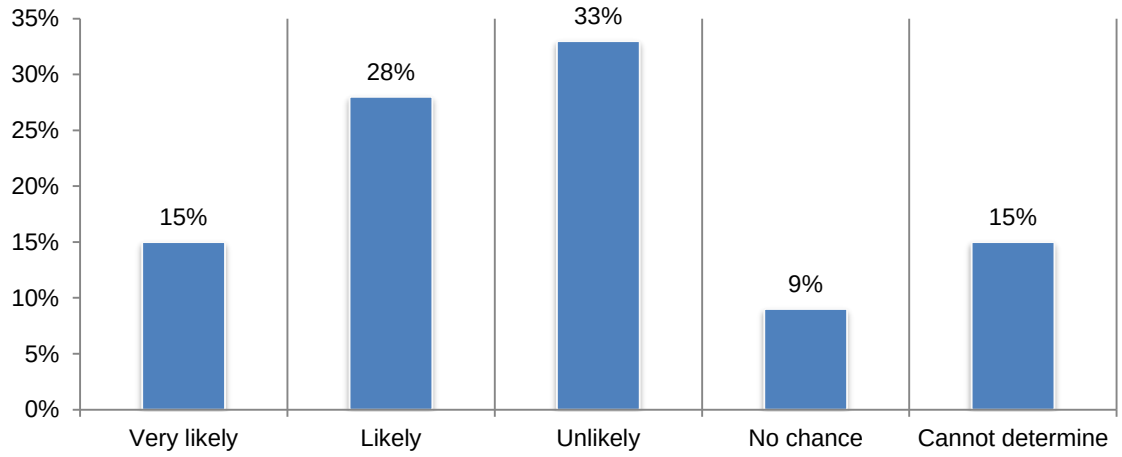
Figure 22. Which department is most likely to execute and take responsibility for the completion of a risk assessment?



If the assessment revealed a lack of controls, would the organization cease or terminate an agreement? According to Figure 23, one-third of respondents say that it would be unlikely their organization would cease or terminate an agreement with a third party that is unable to meet their control requirements. However, more respondents (43 percent of respondents) say it is very likely or likely the third party would be fired.

Respondents report that on average 33.5 percent of their parties require remediation activities during the on-boarding process.

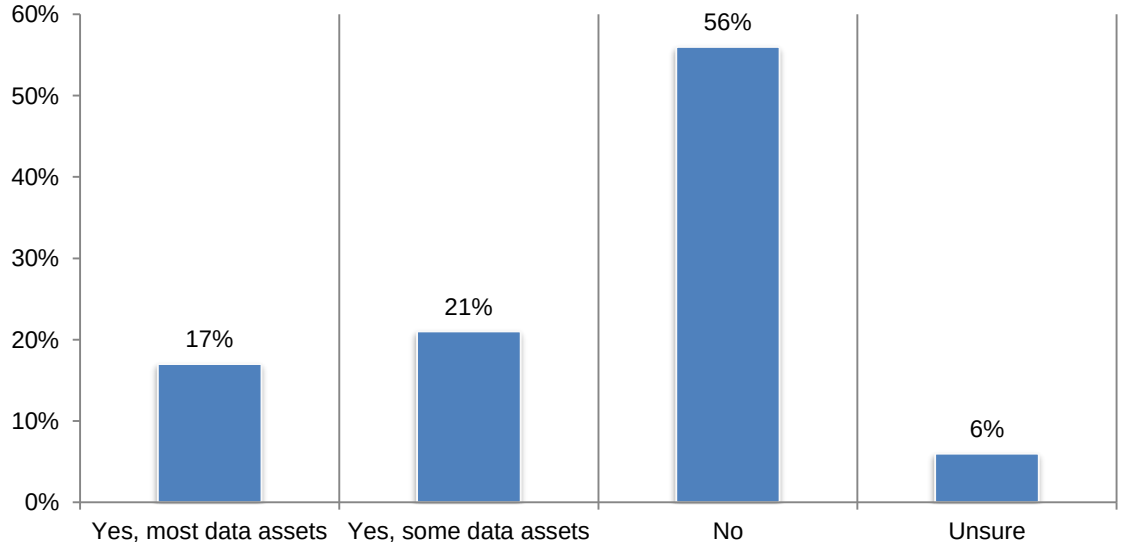
Figure 23. How likely would your organization be to terminate an agreement with a third party with weak controls?



Why is third party risk assessment failing in organizations? Three factors contribute to the ineffectiveness of third party risk assessments.

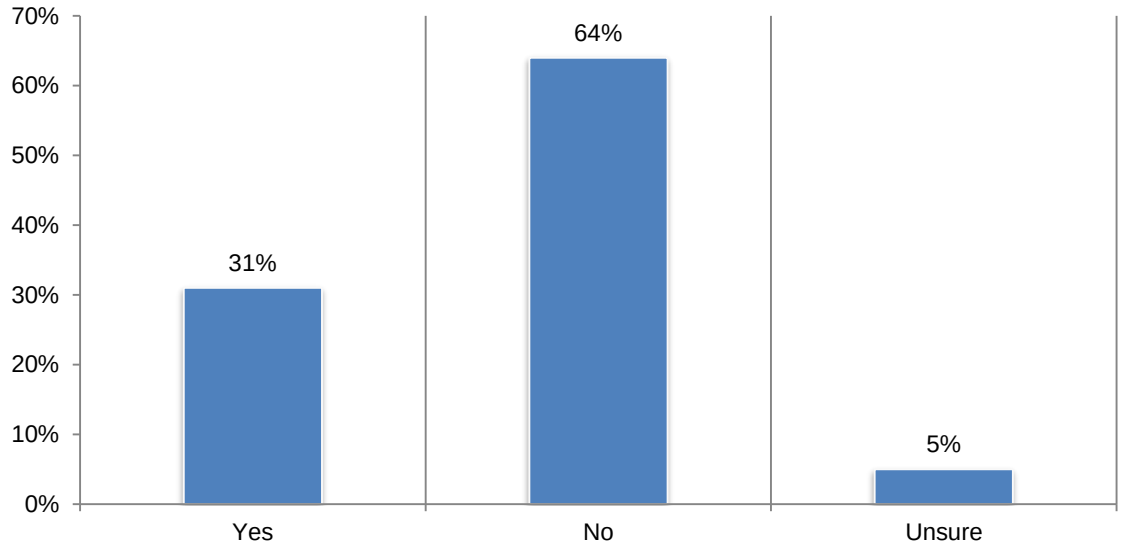
First, 56 percent of respondents say the risk assessment does not reveal the intellectual property (IP) and other high value data that are in the hands of third parties, according to Figure 24.

Figure 24. Does your organization know what high value assets are in the hands of third parties?



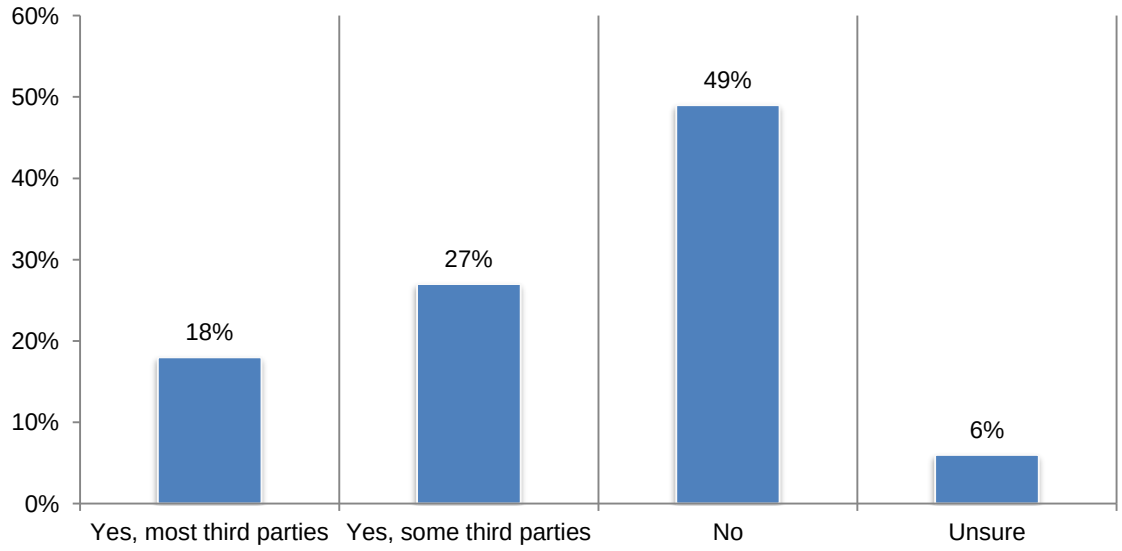
Second, only 31 percent of respondents say they have metrics to measure the effectiveness of risk management activities. As a result, very few organizations in this research are considered to have a highly effective risk management process—probably because they are not attempting to measure its effectiveness, as shown in Figure 25.

Figure 25. Does your organization have metrics to measure the effectiveness of risk management activities?



Third, as shown in Figure 26, only 18 percent of respondents say they assess the cyber security risks of most third parties. Almost half (49 percent of respondents) say they do not conduct such assessments.

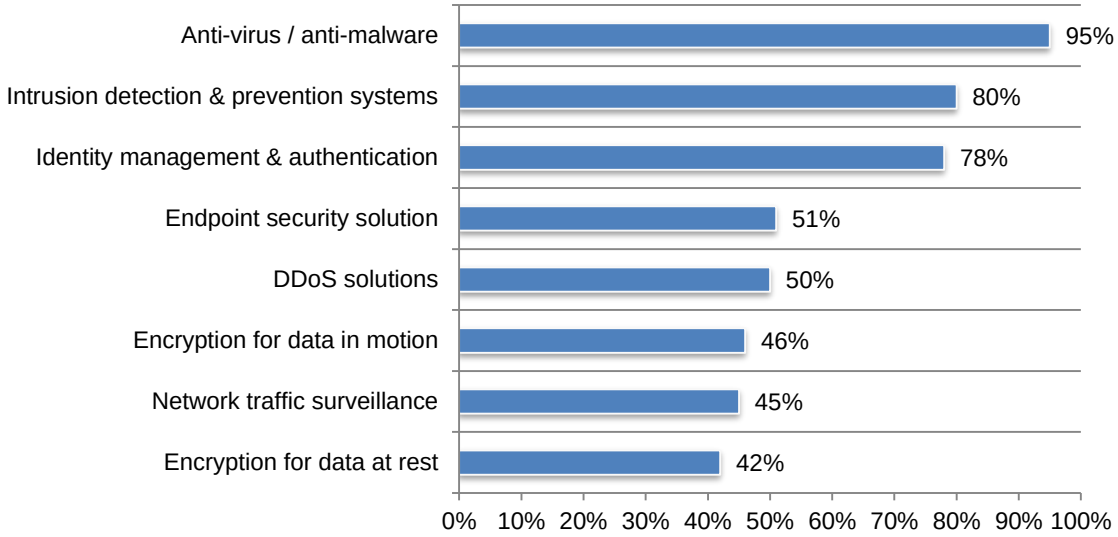
Figure 26. Does your organization assess cybersecurity risk of third parties it deals with?



The use of technologies and cyber insurance to manage third party risk

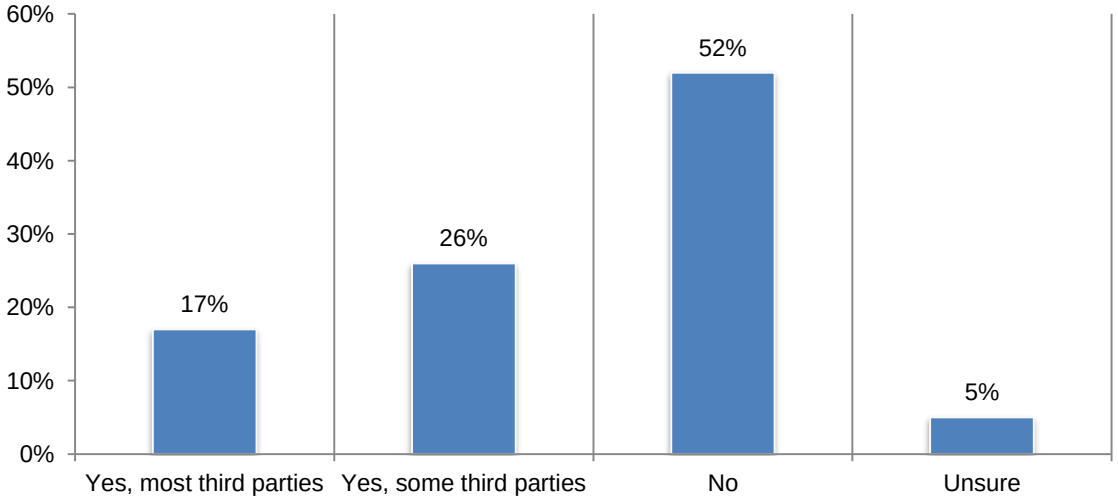
What top technologies do organizations require their third parties to have in place? According to Figure 27, the top three technologies and practices that third parties are expected to have are: anti-virus/anti-malware, intrusion detection and prevention systems and identity management and authentication.

Figure 27. Technologies and practices third parties are expected to have in place to safeguard data.
More than one choice permitted



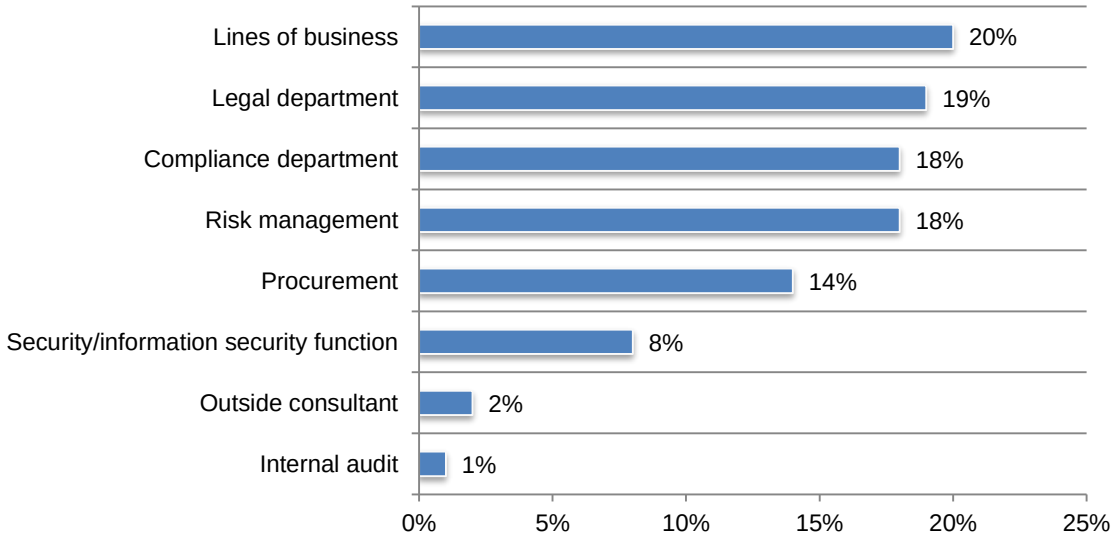
Companies are not procuring cyber insurance to reduce third party risks. While organizations may be purchasing cyber insurance to reduce their own risks, only 26 percent of respondents say they are procuring such insurance to reduce the economic impact of third party risk. As shown in Figure 28, 43 percent of respondents do require most (17 percent of respondents) or some (26 percent of respondents) of business partners, vendors and other third parties to buy such insurance.

Figure 28. Does your organization require third parties to purchase cyber insurance to moderate the economic impact of third party risk?



Lines of business (20 percent of respondents) and the legal department (19 percent of respondents) are most responsible for verifying that the cyber insurance coverage is sufficient for the risk associated with the services received.

Figure 29. Which department verifies that the third party cyber insurance coverage is sufficient?



Conclusion: Ten steps to creating a stronger third party risk management program

The research reveals the gap between the growing increase in third party risk and the lack of a governance strategy to mitigate or curtail the risk. The financial consequences of ignoring the third party risk can be severe. In the past 12 months, organizations represented in this research spent an average of $10 million to resolve the consequences of negligent or malicious third parties. The following are ten steps organizations can take to reduce third party risk.

1. The CEO and boards of directors should be responsible for establishing a positive tone at the top. As shown in the research, a positive tone at the top can improve relationships with third parties and reduce risks.

2. The CEO and boards of directors should become more proactive in the third party risk program. This should include working with management to establish the vision, risk appetite and strategic direction for third party relationships.

3. An organization should communicate its values to employees and other stakeholders through training and policies to ensure enterprise-wide adoption.

4. The business case can be made for dedicating more resources to third party risk management by estimating the potential costs to your organization due to negligent or malicious third parties.

5. The potential threats posed by such disruptive technologies as the use of Cloud and IoT in third parties should be assessed. The results of such assessments should include recommendations as to what technologies and personnel are needed to minimize the threats.

6. The risk of cyber attacks is increasing for all companies and third parties. When partnering with third parties that have access to sensitive and confidential information, ensure they have appropriate technologies to mitigate the threat.

7. Third party risk-management programs should incorporate metrics that reveal the vulnerabilities created by the third parties in your organization's supply chain.

8. While companies in the research have fairly mature risk management programs, it is not clear whether such programs incorporate a strategy for managing third party risk. Such a strategy should incorporate the people, process and technologies for managing the risk.

9. Assign accountability to ensure that the objectives of the risk management program are accomplished. In this research, no one function owns the third party risk management program.

10. Become involved in a consortium or council dedicated to best practices in addressing third party risks.

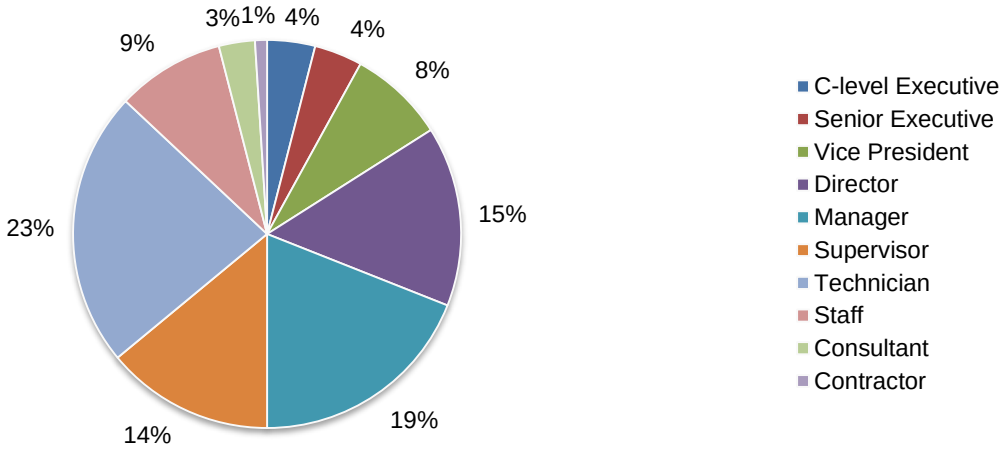
Part 3. Methods

The sampling frame is composed of 17,002 IT and IT security practitioners located in the United States. As shown in Table 1, 676 respondents completed the survey. The screening process removed 59 surveys. The final sample was 617 surveys (or a 3.6 percent response rate).

Table 1. Sample response	Freq
Total sampling frame	17,002
Total returns	676
Rejected or screened surveys	59
Final sample	617
Response rate	3.6%

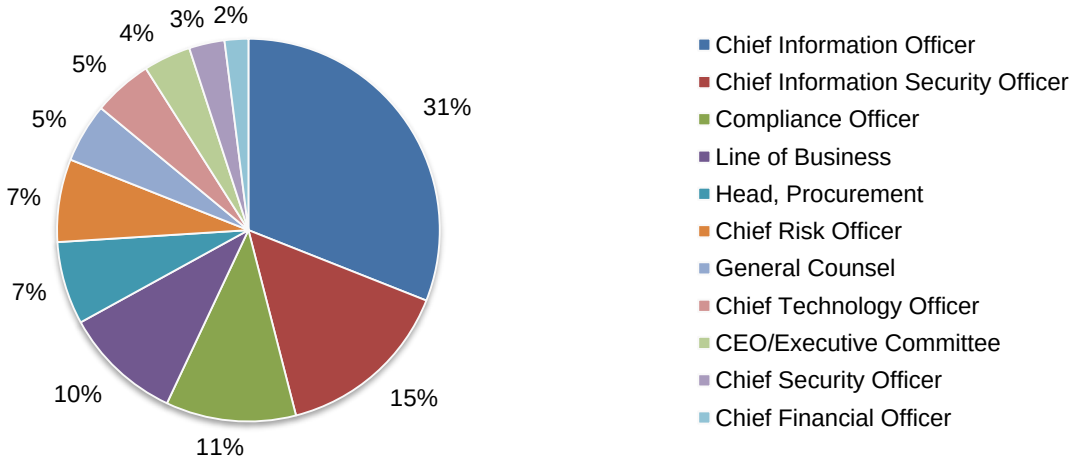
Pie Chart 1 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents (64 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



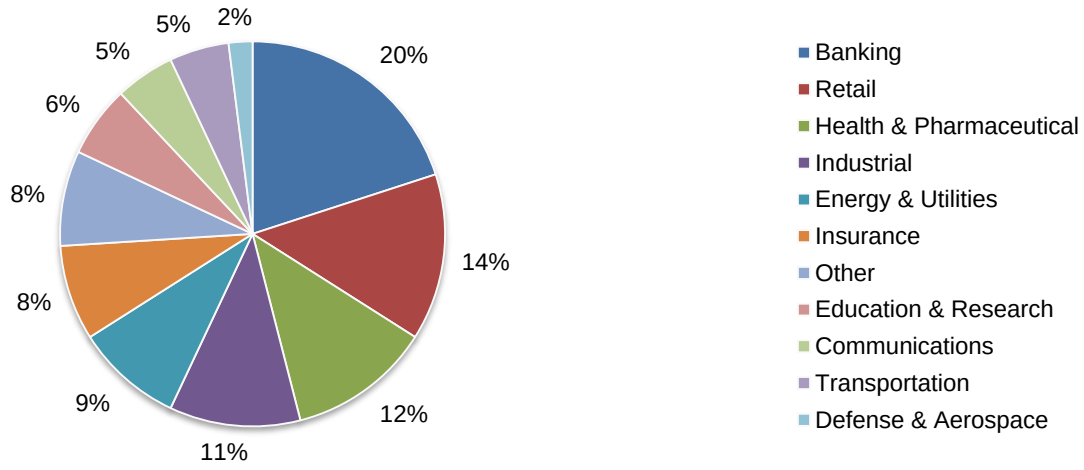
Thirty-one percent of respondents report to the Chief Information Officer, 15 percent report to the Chief Information Security Officer and 11 percent report to the Compliance Officer as shown in Pie Chart 2.

Pie Chart 2. Primary person respondent reports to within the organization



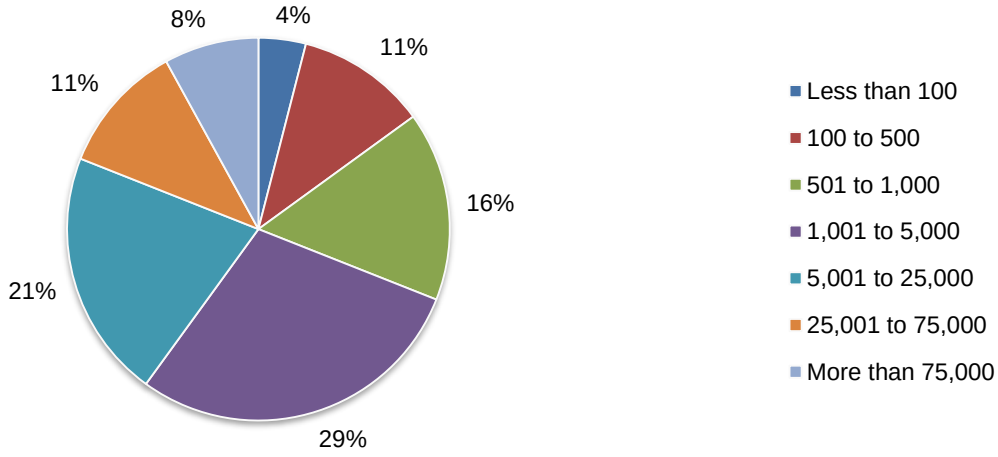
Pie Chart 3 reports the primary industry sector of respondents' organizations. This chart identifies Banking (20 percent) as the largest segment, followed by retail (14 percent) and Health and Pharmaceutical (12 percent).

Pie Chart 3. Primary industry classification



According to Pie Chart 4, the majority of respondents (69 percent) are from organizations with a global headcount of 1,000 or more employees.

Pie Chart 4. Worldwide headcount of the organization



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 who are IT or IT security practitioners located in the United States. We also acknowledge that the results may be biased by external events, such as media coverage.

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 2016.

Survey response	Freq
Total sampling frame	17,002
Total returns	676
Rejected or screened surveys	59
Final sample	617
Response rate	3.6%

Screening

S1. Which of the following best describes your role in the risk management process within your organization? Please check all that apply.	Pct%
Setting priorities	48%
Managing budgets	45%
Evaluating vendors and contractors	65%
Selecting vendors and contractors	61%
Determining risk strategy	28%
Appraising program performance	46%
Enhancing security safeguards	33%
Other (please specify)	3%
None of the above (stop)	0%
Total	329%

S2. How familiar are you with the management of third party risks within your organization?	Pct%
Very familiar	32%
Familiar	40%
Somewhat familiar	28%
Not familiar (stop)	0%
Total	100%

Part 1. Attributions

Q1a. Our organization considers third party risk a serious risk.	Pct%
Strongly agree	35%
Agree	40%
Unsure	9%
Disagree	9%
Strongly disagree	7%
Total	100%

Q1b. C-level executives believe they are ultimately accountable for the effectiveness of their organization's third party risk-management process.	Pct%
Strongly agree	16%
Agree	21%
Unsure	28%
Disagree	19%
Strongly disagree	16%
Total	100%

Q1c. The rise of the Internet of Things (IoT) significantly increases third party risk for my organization.	Pct%
Strongly agree	25%
Agree	35%
Unsure	24%
Disagree	13%
Strongly disagree	3%
Total	100%

Q1d. Migration to the Cloud significantly increases third party risk for my organization.	Pct%
Strongly agree	32%
Agree	36%
Unsure	20%
Disagree	8%
Strongly disagree	4%
Total	100%

Q1e. My organization's risk-management process is aligned with its business goals.	Pct%
Strongly agree	23%
Agree	27%
Unsure	18%
Disagree	24%
Strongly disagree	8%
Total	100%

Q1f. A strong tone at the top is essential to mitigating business risk within my organization.	Pct%
Strongly agree	37%
Agree	41%
Unsure	12%
Disagree	6%
Strongly disagree	4%
Total	100%

Q1g. Board-level governance is an essential part of my organization's risk-management program.	Pct%
Strongly agree	20%
Agree	23%
Unsure	25%
Disagree	23%
Strongly disagree	9%
Total	100%

Part 2. Tone at the top

Q2. Using the following 10-point scale, please rate the importance of a positive tone at the top to minimizing business risks within your organization. 1 = not important to 10 = very important.	Pct%
1 or 2	0%
3 or 4	5%
5 or 6	12%
7 or 8	28%
9 or 10	55%
Total	100%
Extrapolated value	8.16

Q3. Using the following 10-point scale, please rate the importance of a positive tone at the top to minimizing third party (supply chain) risks within your organization. 1 = not important to 10 = very important.	Pct%
1 or 2	0%
3 or 4	6%
5 or 6	16%
7 or 8	25%
9 or 10	53%
Total	100%
Extrapolated value	8.00

Q4. How does the tone at the top mitigate third party risk? Please select all that apply.	Pct%
Increases employee and third party awareness of the importance of security, data protection and business resiliency	43%
Incorporates such values as integrity, ethics and trustworthiness in relationships with third parties	66%
Reduces the risks of working with third parties that are not trustworthy	71%
The tone at the top does not mitigate third party risk	13%
Other (please specify)	2%
Total	195%

Q5. Who is most responsible for setting a positive tone for your organization as a whole?	Pct%
Board of directors	12%
Chief executive officer	41%
Chief ethics officer	2%
General counsel	2%
Compliance officer	19%
Director of internal audit	2%
All C-level executives	6%
All supervisory and management-level employees	10%
All employees	5%
Other (please specify)	1%
Total	100%

Q6. How does your organization communicate its values to employees and other stakeholders? Please select all that apply.	Pct%
Code of conduct	65%
Policies	41%
Memos/emails	19%
Training	50%
Staff meetings	11%
On-the-job mentoring	53%
Other (please specify)	2%
Total	241%

Q7. How effective is your organization at communicating its values throughout the enterprise?	Pct%
Very effective	11%
Effective	32%
Not effective	27%
Not communicated	16%
Cannot determine	14%
Total	100%

Q8. How effective is your organization at communicating its values to business partners, vendors and other third parties?	Pct%
Very effective	11%
Effective	29%
Not effective	29%
Not communicated	15%
Cannot determine	16%
Total	100%

Q9. How effective is your organization at assessing the controls business partners, vendors and other third parties have in place to reduce risks?	Pct%
Very effective	6%
Effective	20%
Not effective	29%
Not assessed (skip)	30%
Cannot determine	15%
Total	100%

Q10a. What steps does your organization take to assess the controls business partners, vendors and other third parties have in place to reduce risks?	Pct%
Risk-based assessment	44%
Internal audit	20%
Legal review	55%
Required contract clauses (plus indemnification)	47%
Background checks (of principals)	25%
Other (please specify)	3%
Total	194%

Q10b. If you selected risk-based assessment, what best describes the risk-assessment process?	Pct%
Formal process that is applied consistently across the enterprise	12%
Formal process that is customized for different types of third party relationships	13%
Informal process that is applied consistently across the enterprise	16%
Informal process that is customized for different types of third party relationships	30%
Ad hoc process	29%
Total	100%

Q10c. If you selected risk-based assessment, which department is most likely to **execute** the risk-based assessment process?	Pct%
Risk management	4%
Business continuity	0%
Procurement	11%
Internal audit	13%
Outside consultant	8%
Legal department	10%
Compliance department	23%
Security/information security function	19%
Lines of business	12%
Ethics office	0%
Privacy office	0%
Other (please specify)	0%
Total	100%

Q10d. If you selected risk-based assessment, which department is most likely to take **responsibility** that it is completed and all risks are addressed?	Pct%
Risk management	5%
Business continuity	0%
Procurement	4%
Internal audit	3%
Outside consultant	2%
Legal department	9%
Compliance department	32%
Security/information security function	18%
Lines of business	27%
Ethics office	0%
Privacy office	0%
Other (please specify)	0%
Total	100%

Q11. Does the board of directors engage in any of the following activities? (please select all that apply)	Pct%
Work with management to establish the vision, risk appetite and overall strategic direction for third party relationships	25%
Oversee the deployment of risk management plans	29%
Review management's analysis of the effectiveness of risk assessment	52%
Review opinions on the results issued by independent risk management or internal audit functions	40%
Review the results of management's ongoing monitoring of the organization's exposure to and preparedness to mitigate third party risk	27%
Review and approve plans to address any risk management or control weaknesses	48%
Other	3%
None of the above	33%
Total	257%

Q12. Using the following 10-point scale, please rate the effectiveness of risk assessments at determining the control environment of business partners, vendors and other third parties. 1 = not effective to 10 = very effective.	Pct%
1 or 2	11%
3 or 4	36%
5 or 6	26%
7 or 8	23%
9 or 10	4%
Total	100%
Extrapolated value	4.96

Q13. How likely would your organization be to cease or terminate an agreement with a third party that is unable to meet your control requirements?	Pct%
Very likely	15%
Likely	28%
Unlikely	33%
No chance	9%
Cannot determine	15%
Total	100%

Q14. Approximately what percentage of your third parties require remediation activities during the on-boarding process in order to meet your control requirements?	Pct%
None	15%
Less than 10%	12%
10% to 20%	10%
21% to 30%	8%
31% to 40%	9%
41% to 50%	12%
More than 50%	34%
Total	100%
Extrapolated value	33.5%

Q15. What best describes the board of directors' level of involvement in overseeing risk management activities?	Pct%
Significant involvement	17%
Some involvement	23%
Limited involvement	26%
No involvement	22%
Do not know	12%
Total	100%

Q16. Does your organization provide a path for employees who are witnessing unethical behavior to be able to report such behavior without fear of retaliation and guaranteed anonymity?	Pct%
Yes	56%
No	30%
Unsure	14%
Total	100%

Q17. Does your organization provide a path for business partners, vendors and other third parties who are witnessing unethical behavior to be able to report such behavior without fear of retaliation?	Pct%
Yes	53%
No	32%
Unsure	15%
Total	100%

Part 3. Third party risk management

Q18. Does your organization have a program for managing third party risks?	Pct%
Yes, a formal program	29%
Yes, an informal program	44%
No (skip)	27%
Total	100%

Q19. Using the following 10-point scale, please rate your organization's effectiveness in mitigating or curtailing third party risk.1 = not effective to 10 = very effective.	Pct%
1 or 2	24%
3 or 4	37%
5 or 6	18%
7 or 8	12%
9 or 10	9%
Total	100%
Extrapolated value	4.40

Q20. What best describes the maturity level of your organization's risk management program or activities?	Pct%
Non-existent	6%
Initial visioning	8%
Determining road map to achieve success	11%
Fully determined and established	33%
Fully implemented and operational	25%
Continuous improvement	17%
Total	100%

Q21. What are the top two risk-management objectives within your organization?	Pct%
Prevent cyber attacks	27%
Minimize downtime	56%
Minimize business disruptions	37%
Comply with regulations and legal mandates	23%
Protect intellectual properties (trade secrets)	15%
Secure the national critical infrastructure	9%
Improve the organization's relationship with business partners	8%
Preserve brand and reputation	23%
Other (please specify)	2%
Total	200%

Q22. Which department is most likely to **own** third party risk management in your organization?	Pct%
Risk management	9%
Business continuity	0%
Procurement	15%
Internal audit	3%
Outside consultant	2%
Legal department	15%
Compliance department	23%
Security/information security function	17%
Lines of business	14%
Ethics office	2%
Privacy office	0%
Other (please specify)	0%
Total	100%

Q23. In your opinion, is third party risk within your organization increasing, decreasing or staying at about the same level?	Pct%
Significantly increasing	21%
Increasing	20%
Staying the same	29%
Decreasing	13%
Significantly decreasing	6%
Cannot determine	11%
Total	100%

Q24. Using the following 10-point scale, please rate the impact of the **Internet of Things (IoT)** on your organization's third party risk profile.1 = no impact to 10 = significant impact.	Pct%
1 or 2	5%
3 or 4	7%
5 or 6	12%
7 or 8	36%
9 or 10	40%
Total	100%
Extrapolated value	7.48

Q25. Using the following 10-point scale, please rate the impact of **Cloud computing** on your organization's third party risk profile.1 = no impact to 10 = significant impact.	Pct%
1 or 2	1%
3 or 4	6%
5 or 6	22%
7 or 8	40%
9 or 10	31%
Total	100%
Extrapolated value	7.38

Q26. Using the following 10-point scale, please rate the impact of **mobility and mobile devices** on your organization's third party risk profile.1 = no impact to 10 = significant impact.	Pct%
1 or 2	2%
3 or 4	8%
5 or 6	23%
7 or 8	39%
9 or 10	28%
Total	100%
Extrapolated value	7.16

Q27. Using the following 10-point scale, please rate the impact of **cyber attacks** on your organization's third party risk profile.1 = no impact to 10 = significant impact.	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	19%
7 or 8	29%
9 or 10	49%
Total	100%
Extrapolated value	7.98

Q28. Using the following 10-point scale, please rate the impact of **big data analytics** on your organization's third party risk profile.1 = no impact to 10 = significant impact.	Pct%
1 or 2	4%
3 or 4	7%
5 or 6	38%
7 or 8	41%
9 or 10	10%
Total	100%
Extrapolated value	6.42

Q29. What technologies and practices would you expect your third party to have in place to protect your company's sensitive or confidential information? Please select all that apply from the following list.	Pct%
Anti-virus / anti-malware	95%
Intrusion detection & prevention systems	80%
Identity management & authentication	78%
Endpoint security solution	51%
DDoS solutions	50%
Encryption for data in motion	46%
Network traffic surveillance	45%
Encryption for data at rest	42%
Continuous monitoring	39%
Onsite assessments	38%
Virtual private networks (VPN)	35%
Data loss prevention (DLP)	31%
Security information and event management (SIEM)	20%
Data tokenization technology	20%
Wireless security solutions	19%
Governance solutions (GRC)	17%
Web application firewalls (WAF)	12%
Code review and debugging systems	12%
Next generation firewalls	10%
Big data analytics for cyber security	9%
Other (please specify)	5%
Total	754%

Q30a. Does your organization procure cyber insurance to mitigate the economic impact of third party risk?	Pct%
Yes	26%
No	69%
Unsure	5%
Total	100%

Q30b. If yes, does your organization require business partners, vendors and other third parties to procure cyber insurance to moderate the economic impact of third party risk?	Pct%
Yes, most third parties	17%
Yes, some third parties	26%
No	52%
Unsure	5%
Total	100%

Q30c. If yes, which department within your organization verifies that the cyber insurance coverage is sufficient for the risk associated with the services received?	Pct%
Risk management	18%
Procurement	14%
Internal audit	1%
Outside consultant	2%
Legal department	19%
Compliance department	18%
Security/information security function	8%
Lines of business	20%
Ethics office	0%
Privacy office	0%
Other (please specify)	0%
Total	100%

Q31. Approximately, what is the total cost impact your organization suffered as a result of negligent or malicious third parties (over the past 12 months)?	Pct%
Zero	0%
Less than $100,000	1%
$100,001 to $250,000	8%
$250,001 to $500,000	10%
$500,001 to $1,000,000	15%
$1,000,001 to $5,000,000	17%
$5,000,001 to $10,000,000	15%
$10,000,001 to $25,000,000	13%
$25,000,001 to $50,000,000	5%
$50,000,001 to $100,000,000	2%
More than $100,000,000	1%
Cannot estimate	13%
Total	100%
Extrapolated value	$9,942,414

Q32. Does your organization know what intellectual property (IP) and other high value data assets are in the hands of third parties?	Pct%
Yes, most data assets	17%
Yes, some data assets	21%
No	56%
Unsure	6%
Total	100%

Q33. Does your organization have metrics to measure the effectiveness of risk management activities?	Pct%
Yes	31%
No	64%
Unsure	5%
Total	100%

Q34. Does your organization assess cybersecurity risk of third parties it deals with?	Pct%
Yes, most third parties	18%
Yes, some third parties	27%
No	49%
Unsure	6%
Total	100%

Part 4. Your role and organization

D1. What organizational level best describes your current position?	Pct%
C-level Executive	4%
Senior Executive	4%
Vice President	8%
Director	15%
Manager	19%
Supervisor	14%
Technician	23%
Staff	9%
Consultant	3%
Contractor	1%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/Executive Committee	4%
Chief Financial Officer	2%
General Counsel	5%
Chief Information Officer	31%
Chief Technology Officer	5%
Chief Information Security Officer	15%
Compliance Officer	11%
Line of Business	10%
Head, Procurement	7%
Chief Security Officer	3%
Chief Risk Officer	7%
Total	100%

D3. What industry best describes your organization's industry focus (stratified list)?	Pct%
Communications	5%
Defense & Aerospace	2%
Education & Research	6%
Energy & Utilities	9%
Banking	20%
Insurance	8%
Health & Pharmaceutical	12%
Industrial	11%
Retail	14%
Transportation	5%
Other	8%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 100	4%
100 to 500	11%
501 to 1,000	16%
1,001 to 5,000	29%
5,001 to 25,000	21%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

The Shared Assessments Program is the trusted source in third party risk management, with resources to effectively manage the critical components of the vendor risk management lifecycle that are: creating efficiencies and lowering costs for all participants; kept current with regulations, industry standards and guidelines, and the current threat environment; and adopted globally across a broad range of industries both by service providers and their customers. Shared Assessments membership and use of the Shared Assessments Program Tools: Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means of conducting rigorous assessments of controls for IT and data security, privacy and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

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.