The Economic Impact of Third-Party Risk Management in Healthcare

Sponsored by Censinet

Independently conducted by Ponemon Institute LLC

Publication Date: July 2019

The Economic Impact of Third-Party Risk Management in Healthcare

Prepared by Ponemon Institute, July 2019

Part 1. Introduction

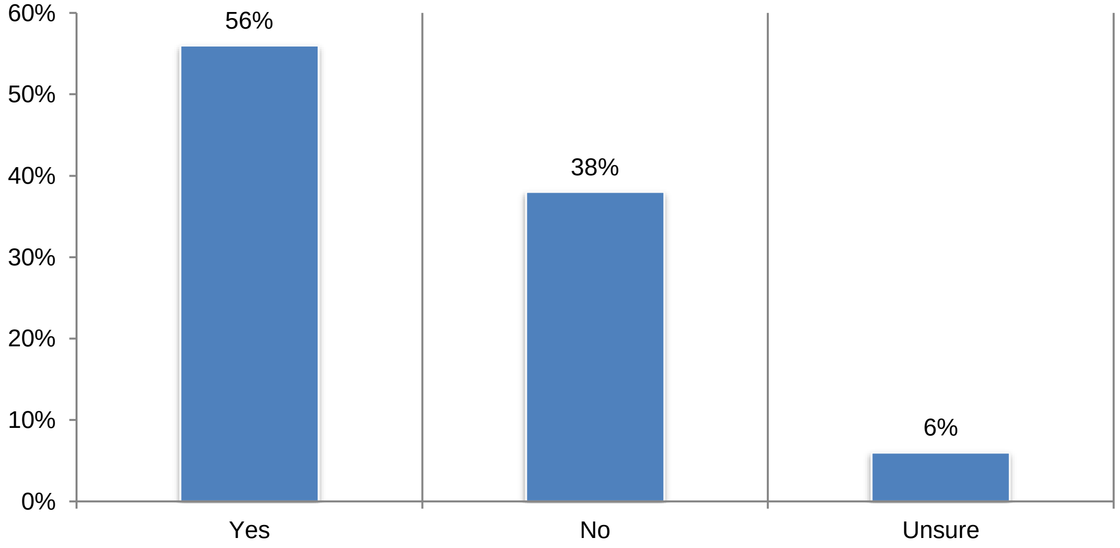
Healthcare organizations are struggling to prevent or mitigate the severity of a third-party or vendor-related data breach. However, as shown in this report, current approaches to assessing and managing vendor risks are failing. Problems with current approaches to third-party risk management are creating a real economic impact as these organizations are seeing an increase in HHS and OCR fines and investigations. Following are some of the reasons why third-party risk management programs are failing in healthcare.

- The lack of automation and reliance upon manual risk management processes makes it difficult to keep pace with cyber threats and the proliferation of digital applications and medical devices used in healthcare.
- Vendor risk assessments are time-consuming and costly so few organizations are conducting risk assessment of **all** their vendors. Currently, an average of 3.21 full-time employees are fully dedicated to completing vendor risk assessments and they spend an average of 513 hours monthly to complete these assessments. This represents approximately 10 percent of the total hours expended on third-party supply chain activities.
- The indirect and direct costs of third-party risk management for the healthcare industry averages $23.7 billion annually.
- Critical vendor management controls and processes are often only partially deployed or not deployed at all. If controls and processes are deployed, they are not considered very effective in reducing third-party risks.

Ponemon Institute surveyed 554 IT and IT security professionals in healthcare companies who are involved in managing their organizations' vendor risk management programs (VRMP). All organizations represented in the study have VRMPs.

Organizations are having multiple and costly data breaches caused by their vendors. Healthcare organizations are vulnerable to security exploits because of the inability to adequately assess and understand vendor risks. As shown in Figure 1, the majority of organizations have had one or more data breaches caused by one of their vendors and the average cost of these vendor-related data breaches was $2.9 million.

Figure 1. Did your organization have one or more third-party data breaches over the past two years?



Following are important findings from this research.

Only one-third of healthcare organizations in this research automate most of their vendor assessment programs. Reliance on manual processes makes it difficult for organizations to assess all their vendors and to understand the types of vendor risk they face. Respondents believe it is very important to understand the potential financial risk and potential legal and regulatory risk of vendors. Understanding the information security risks, resiliency and availability of vendors is also very important.

Respondents recognize the importance of automation. Seventy-eight percent of respondents say it is very important to be able to continuously update changes to third-party risk, 74 percent of respondents say it is very important to have a standardized vendor assessment questionnaire and 72 percent of respondents say it is very important to be able to access vendor assessments and supporting evidence easily and immediately.

Most organizations do not find the information from vendor assessments valuable. Only 40 percent of respondents say vendor assessments are very valuable in terms of providing actionable insights that can be reported to the C-suite and board of directors. Forty-two percent say these assessments are somewhat valuable in providing information on what actions their organization should take.

Organizations are not requiring remediation or disqualification when an assessment reveals security gaps. Only an average of 21 percent of all assessments result in a requirement to remediate prior to doing business with them and only 11 percent of respondents say they result in disqualification.

Moreover, vendor's security gaps are not addressed following an assessment. Respondents were asked what they do if they determine working with the vendor will put their organizations at risk. Only one-third of respondents say they would mitigate or remediate the security gap and only 28 percent of respondents say they would terminate the relationship with the vendor. These findings indicate that most organizations might not have processes in place to follow-up when such security gaps are revealed.

Organizations are not allocating sufficient budget to have an effective vendor-risk management program. The average annual cybersecurity budget for organizations represented in this research is $12.05 million. Fifty-two percent of respondents say their organizations allocate an average of 17 percent of the cybersecurity budget or approximately $2 million for their vendor risk management programs. Respondents estimate it costs an average of $5 million to implement all four controls.

Vendor risk management controls and practices are only partially deployed or not deployed at all. According to the findings, the majority of all data breaches experienced by the organizations in this research are caused by vendors. However, such important controls such as the prioritization of vendor risks and data breach cyber exploit response procedures are rarely fully deployed. Enforcement of non-compliance with security requirements is the control practice most often fully deployed.

Vendor management risk controls are considered important but not considered very effective. While 86 percent say data breach cyber exploit response procedures are very important, only 33 percent of respondents say the practice is very effective. Eighty percent say prioritization of vendor risks is considered very important but only 36 percent of respondents say it is very effective.

Part 2. Key findings

In this section, we present an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The findings are organized by the following themes:

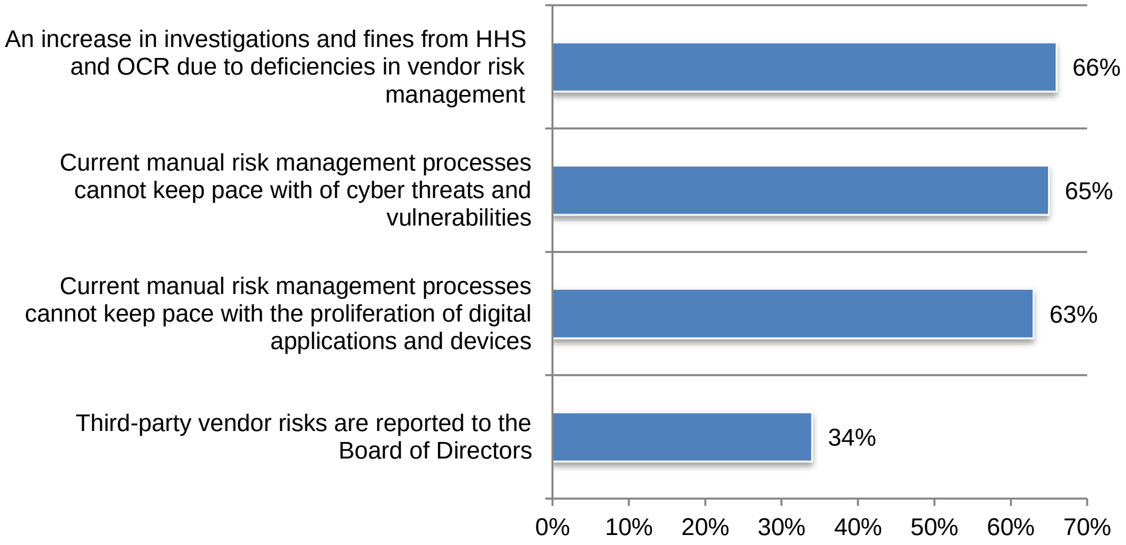
1. Current third-party risk assessments fail to reduce security risks
2. The importance of automation to reducing third-party risks
3. Third-party vendor management controls are costly to deploy and ineffective

1. Current third-party risk assessments fail to reduce security risks

Risk management practices are not keeping pace with third-party security vulnerabilities. According to Figure 2, current manual risk management processes cannot keep pace with cyber threats and vulnerabilities (65 percent of respondents) and with the proliferation of cloud applications and internet-connected devices (63 percent of respondents).

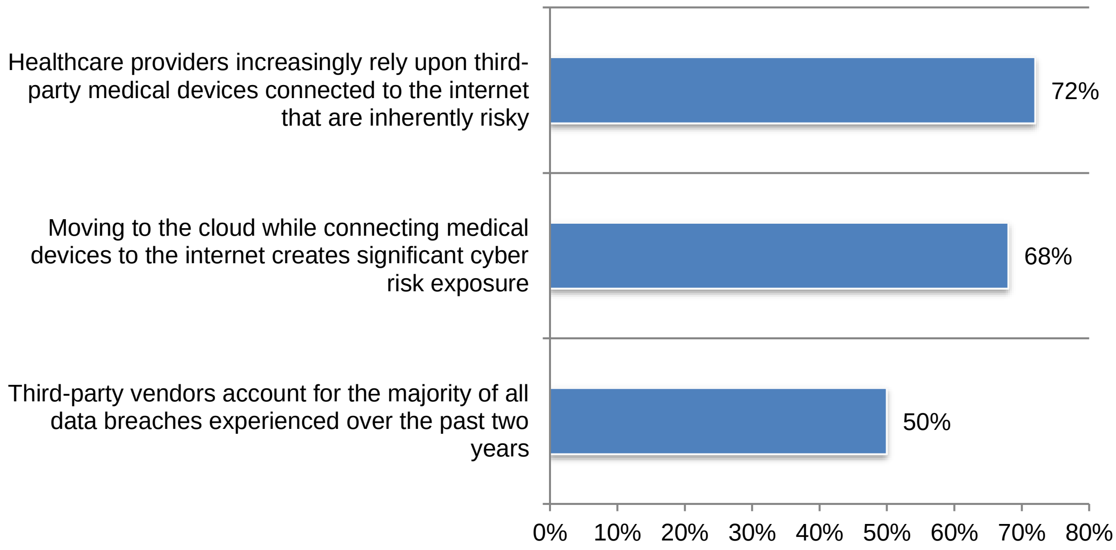
As a result of ineffective manual processes causing deficiencies in managing vendor risks, 66 percent of respondents are seeing an increase in investigations and fines from HHS and the OCR. Another consequence of vendor assessments not providing valuable and actionable insights is that very few boards of directors are briefed on these risks (34 percent of respondents).

Figure 2. Perceptions about third-party vendor risks
Strongly agree and Agree responses combined



The use of medical devices is increasing third-party risk. As shown in Figure 3, 72 percent of respondents say that the increasing reliance upon third-party medical devices connected to the internet are risky and 68 percent of respondents say moving to the cloud while connecting medical devices to the internet creates significant cyber risk exposure.

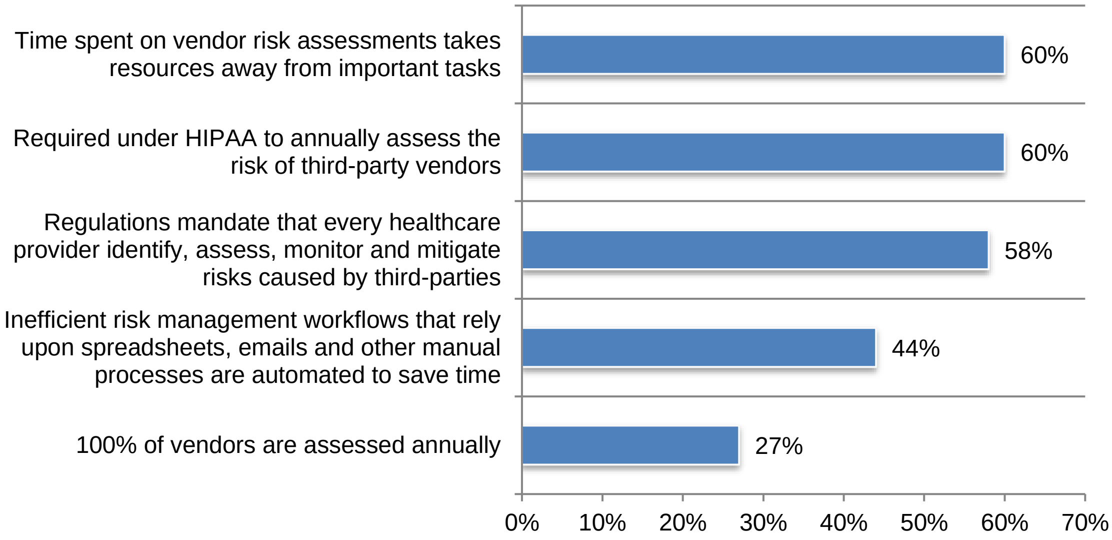
Figure 3. The cloud and Internet increase third-party risks
Strongly agree and Agree responses combined



Most healthcare organizations believe they are required to assess vendor risks. According to Figure 4, 60 percent of respondents believe HIPAA requires annual assessment of third-party risks and 58 percent of respondents say regulations require them to identify, assess and monitor and mitigate risks caused by third parties. However, only 27 percent of respondents say their organizations conduct risk assessments of all their vendors. This gap between what regulations require and what is actually done means that organizations are vulnerable to data breaches and regulatory fines.

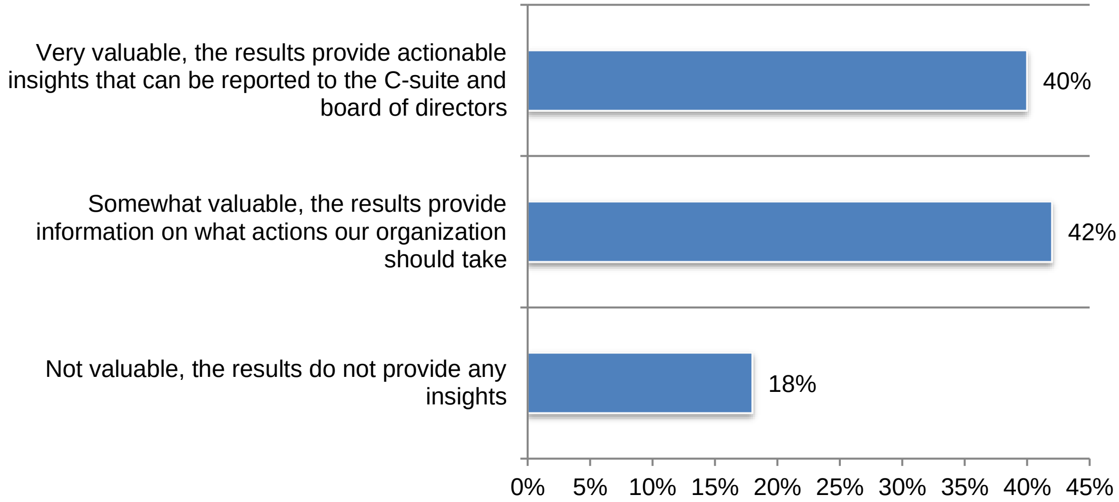
A reason for not assessing all vendors is that respondents believe their current approach to risk assessments takes resources away from other important tasks such as staff training, building controls over data assets, incident response planning and upstream communications.

Figure 4. Perceptions about vendor risk assessments
Strongly agree and Agree responses combined



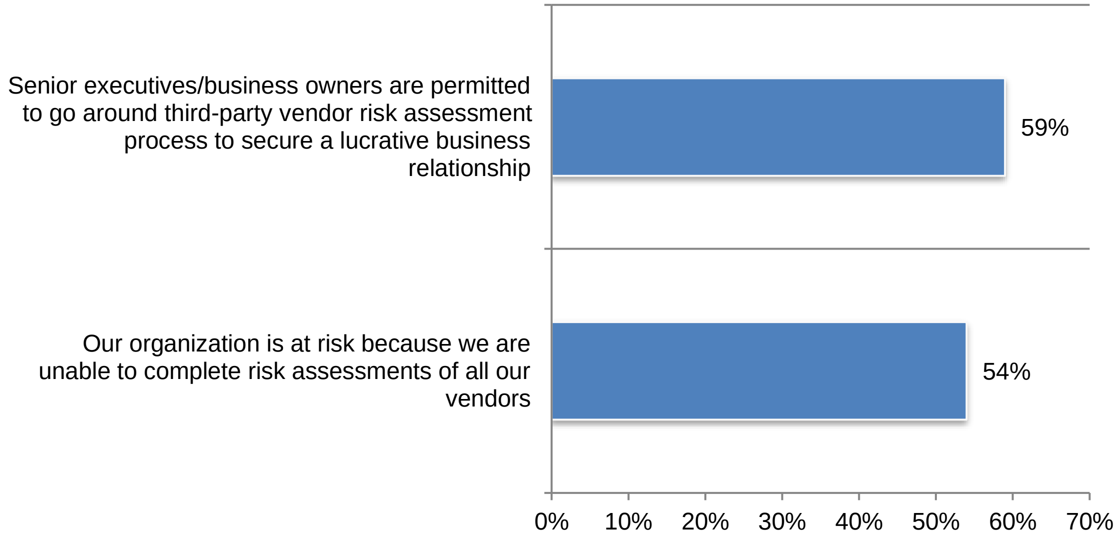
Most organizations do not find the information from vendor assessments valuable. Respondents were asked to rate the value of vendor risk assessments performed by their organization in terms of cost savings and/or risk reduction. As shown in Figure 5, only 40 percent of respondents say such assessments are very valuable in terms of providing actionable insights that can be reported to the C-suite and board of directors. Forty-two percent say these assessments are somewhat valuable in providing information on what actions their organization should take.

Figure 5. How valuable are the results of vendor risk assessments?



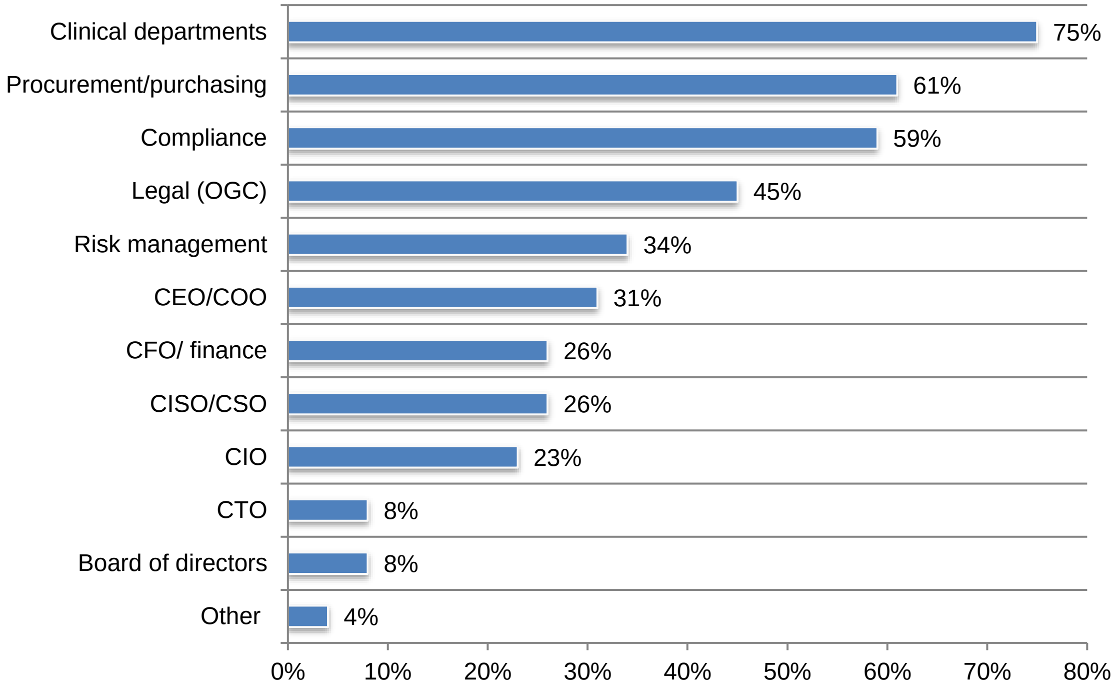
As discussed previously, only 27 percent of respondents say their organizations assess 100 percent of their vendors. Figure 6 reveals why this is the case. According to 59 percent of respondents, senior executives are permitted to avoid conducting an assessment to secure a lucrative business relationship. Fifty-four percent of respondents say they are at risk because they cannot complete all risk assessments.

Figure 6. Not completing all vendor assessments puts organizations at risk
Strongly agree and Agree response combined



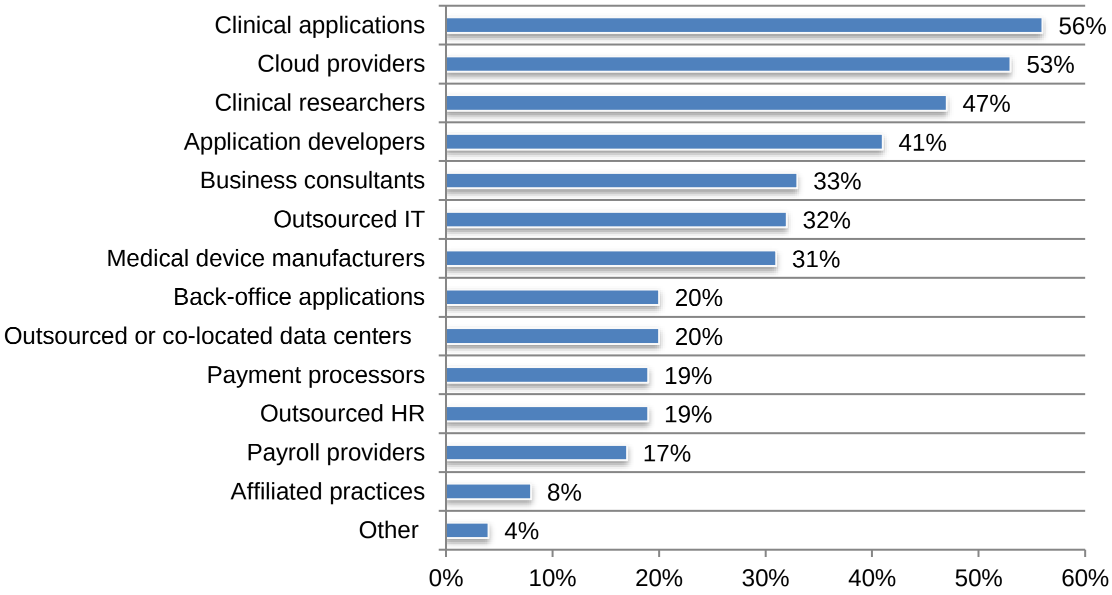
Clinical departments benefit the most from an effective vendor risk management program. According to Figure 7, by far the clinical departments benefit most when vendor risks are identified and remediated followed by purchasing (75 percent and 61 percent of respondents, respectively).

Figure 7. Which function benefits most from a well-functioning vendor risk management process or program?
Three responses permitted



As shown above, clinical departments could benefit the most most from a well-run vendor risk management program. According to Figure 8, the vendors that pose the greatest risk are those that provide clinical applications followed by cloud providers.

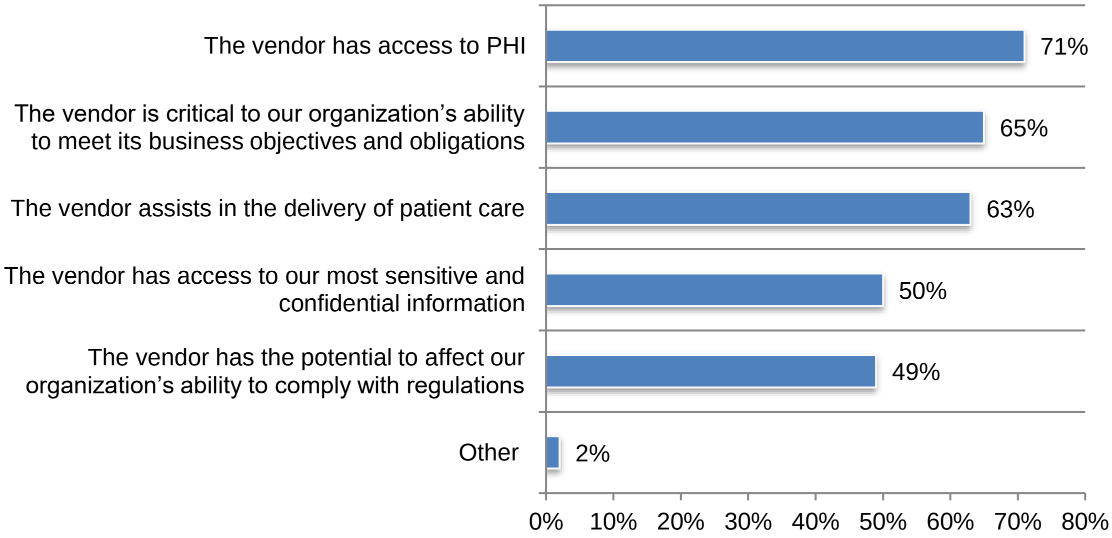
Figure 8. Vendor types that pose the highest risk
Four responses permitted



Organizations are prioritizing the vendors to assess. Healthcare organizations represented in this research say they have an average of 1,320 vendors under contract and only 27 percent of respondents say they conduct vendor assessments for all of them. Instead, 64 percent of respondents say they select certain vendors for a more comprehensive assessment or level of due diligence than others.

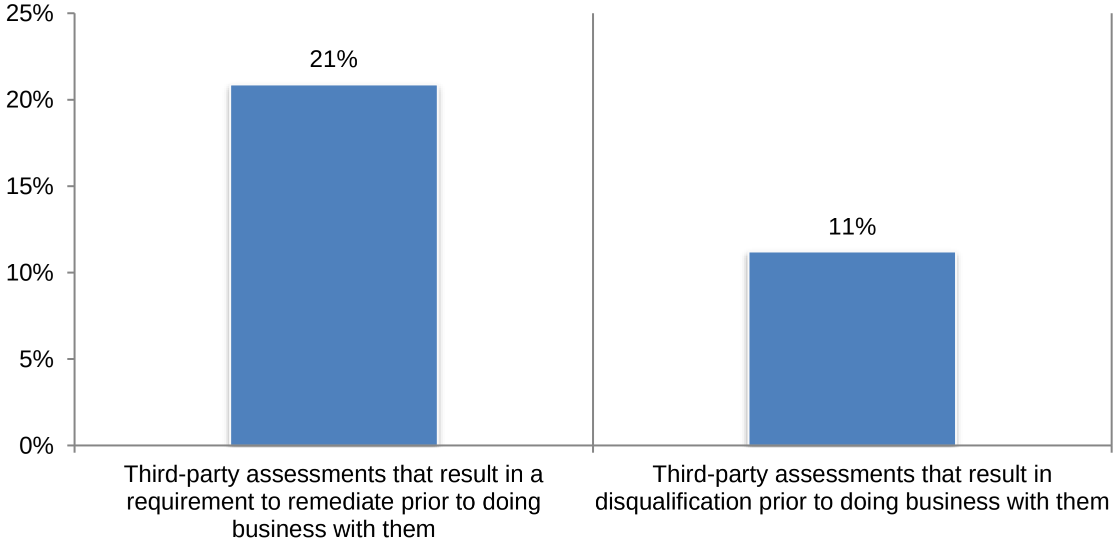
Of these respondents, 71 percent say they are assessed if they have access to PHI and 65 percent of respondents say it is because the vendor is critical to their ability to meet its business goals. Despite the increase in investigations and fines for non-compliance, less than half of respondents (49 percent) assess based on the possibility the vendor will affect their ability to comply with regulations, as shown in Figure 9.

Figure 9. How do you determine which vendors to prioritize for due diligence and assessment?
Three responses permitted



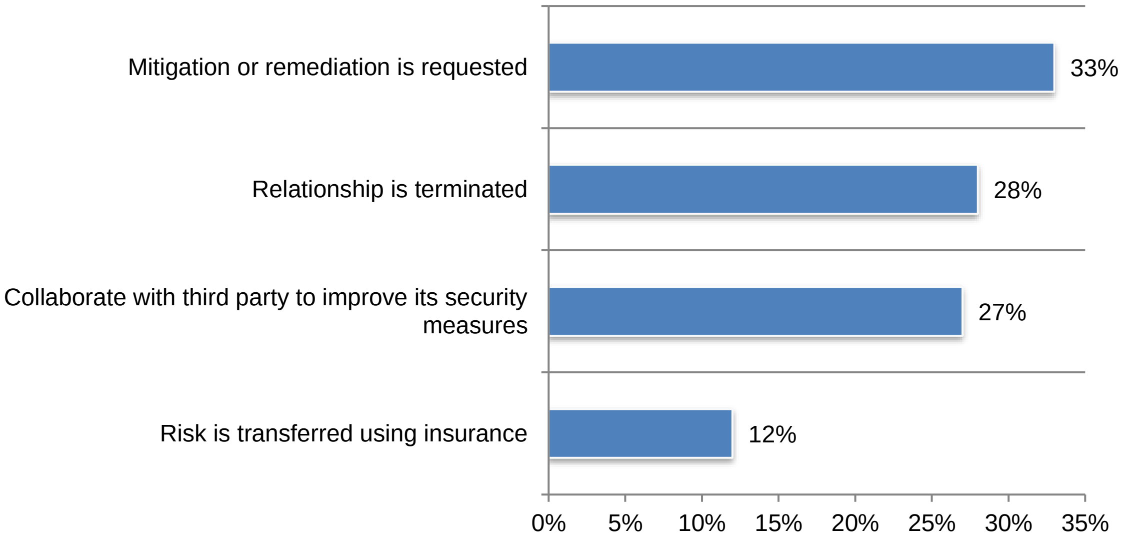
Organizations are not requiring remediation or disqualification when an assessment reveals security gaps. Figure 10 reveals problems with vendor risk management practices. Specifically, only an average of 21 percent of all assessments result in a requirement to remediate prior to doing business with them and only 11 percent of respondents say they result in disqualification.

Figure 10. The percent of vendor assessments that result in disqualification or requirement to remediate
Extrapolated values presented



Vendor's security gaps are not addressed following an assessment. Respondents were asked what they do if they determine working with the vendor will put their organizations at risk. As shown in Figure 11, only one-third of respondents say they would mitigate or remediate the security gap and only 28 percent of respondents say they would terminate the relationship with the vendor.

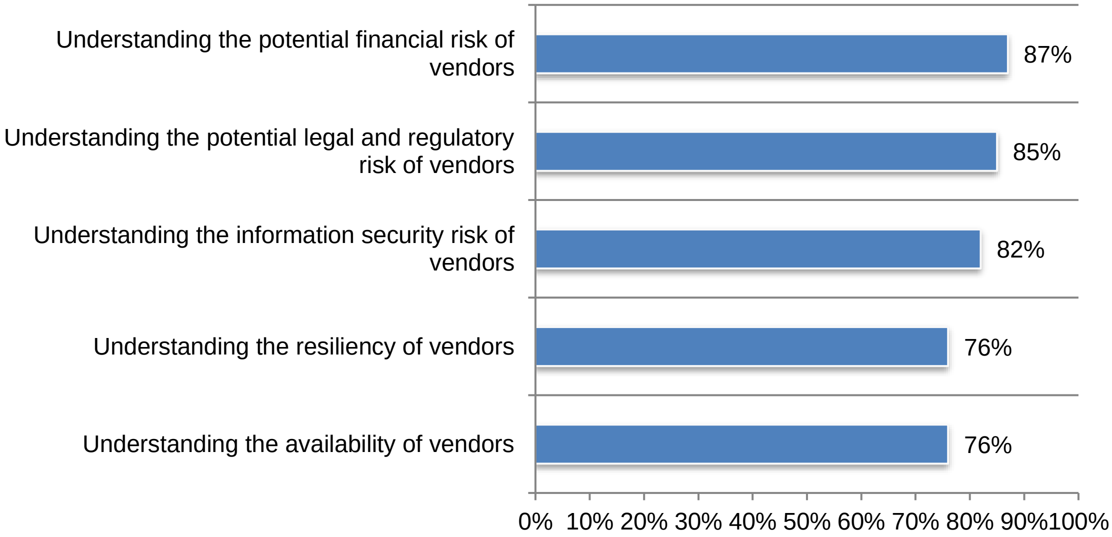
Figure 11. What actions does your organization take if the vendor has security gaps?



2. The importance of automation to reducing third-party risks

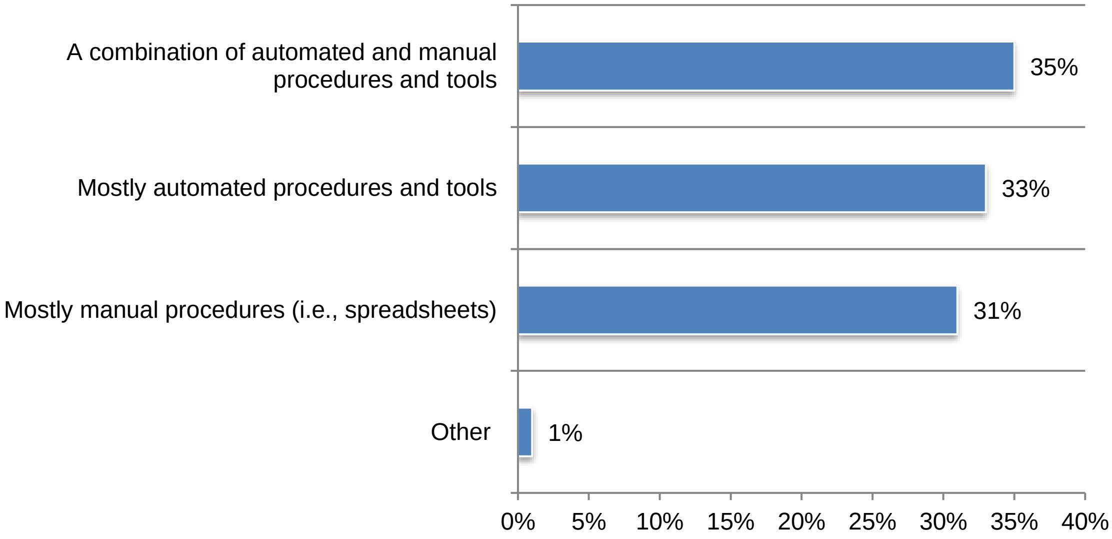
Reliance on manual processes make it difficult to understand all vendor risks facing the organization. Respondents were asked to rate the importance of understanding a variety of vendor risks on a scale of 1 = not important to 10 = very important. Figure 12, presents the very important responses for five areas of vendor risk. The most important are potential financial and legal and regulatory risks, according to 87 percent and 85 percent of respondents respectively.

Figure 12. The importance of understanding vendor risk
On a scale from 1 = not important to 10 = very important, 7+ responses reported



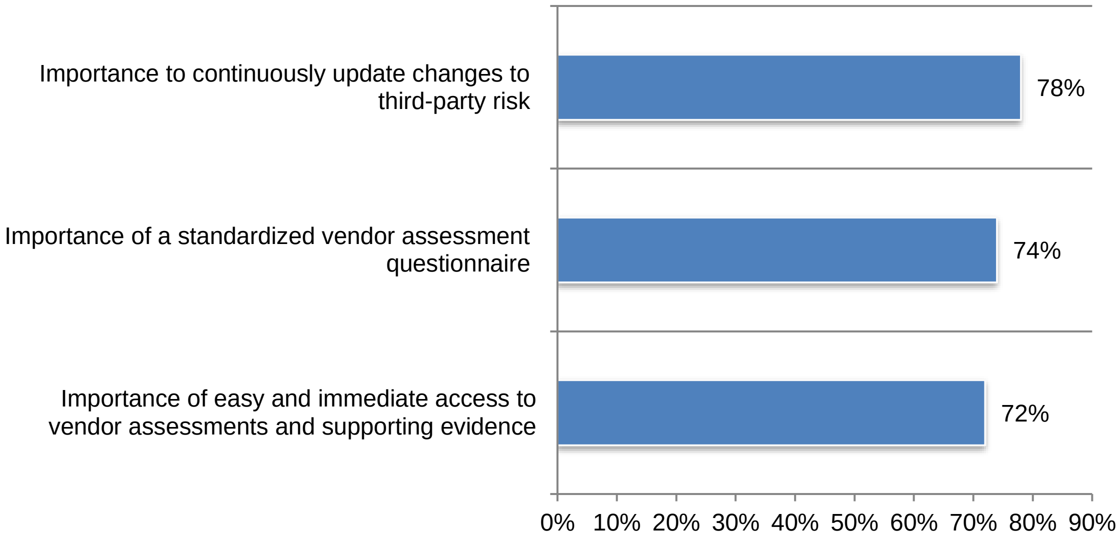
Only one-third of respondents are automating most of their vendor assessment programs. Respondents were asked to identify the one tool their organizations primarily use to assess vendor risk. According to Figure 13, 35 percent of respondents say a combination of automated and manual procedures and tools are used and 31 percent of respondents say assessments are manual.

Figure 13. Tools used to assess vendor risk



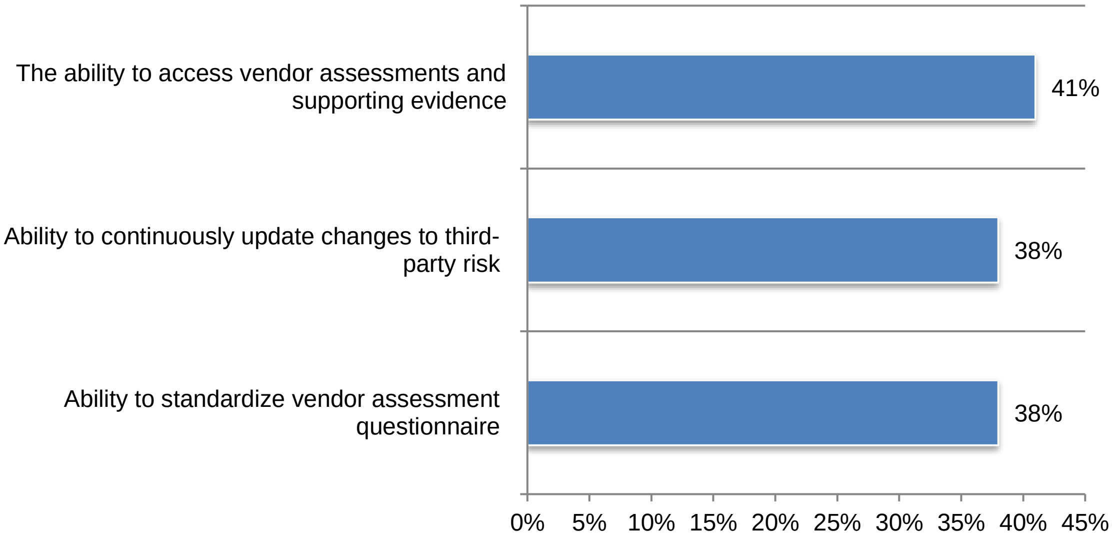
Automation features are considered very important. Respondents were asked to rate the importance of specific features of automation risk management tools on a scale of 1 = not important to 10 = very important. Most respondents understand the importance of continuously updating changes to third-party risk, having a standardized assessment questionnaire and being able to have easy and immediate access to vendor assessments and supporting evidence, as shown in Figure 14.

Figure 14. Importance of automated risk management features
On a scale from 1 = Not important to 10 = Very important
7+ responses presented



However, most respondents do not have the ability to achieve the goals of automation they believe are important. When asked to rate their ability on a scale of 1 = low ability to 10 = high ability, only 38 percent of respondents say they are able to continuously update changes to third-party risk and to have a standardized assessment questionnaire.

Figure 15. Ability to achieve automated risk management features
On a scale from 1 = Low ability to 10 = High ability
7+ responses presented



3. The economic impact of third-party risk management controls

In this section we present the extrapolated labor cost impact of third-party risk management for registered hospitals in the United States. The first analysis presents the direct labor cost impact. As shown in Table 1, survey results provide an estimate of 3.2 full-time equivalent (FTE) employees dedicated to third-party risk management activities.

Calculus	Source	Direct labor costs
Average number of FTEs	Survey Q	3.2
Hourly capacity of dedicated FTEs per week	Calc: 3.2 FTE x 40	128
Hourly capacity of dedicated FTEs per month	Calc: 128 hrs x 4 weeks	514
Hourly capacity of dedicated FTEs per year	Calc: 514 hrs x 12 months	6,163
Number of registered hospitals in the US	2019 AHA Hospital Statistic	6,210
Total direct hours for US hospital industry per year	Calc: 6,163 hrs x 6,210	38,273,472
Fully loaded labor cost per hour	Benchmark for healthcare providers	$ 63
Direct annual labor cost for US hospital industry	Calc: 38.3 million hrs x $63	$2.4 billion

Assuming a capacity of 40 hours per week, we estimated 512 hours per month or 6,163 hours per year dedicated to third-party risk management. Using the 2019 AHA estimate of 6,210 registered U.S. hospitals, we compute 38.3 million hours for the entire industry each year. We also assume a fully loaded labor cost of $63 per hour, which is based on benchmarks compiled by Ponemon Institute for U.S.-healthcare personnel in IT, administration and clinical management. Multiplying total direct labor hours by the estimated labor rate, we compute a total industry impact of $2.4 billion dollars per annum.

The second analysis provides the combined direct and indirect labor cost impact, which includes the hours of individuals who are not dedicated to vendor risk management, but who are involved in a wide array of supply chain activities that touch third-party management and oversight.

Calculus	Source	Direct and indirect labor costs
Total hours per month expended by all employees	Survey Q	5,040
Total hours per year expended by all employees	Calc: 5,040 hrs x 12 months	60,480
Number of registered hospitals in the US	2019 AHA Hospital Statistic	6,210
Total hours for US hospital industry per year	Calc: 60,480 hrs x 6,210	375,580,800
Fully loaded labor cost per hour	Benchmark for healthcare providers	$ 63
Total annual labor cost for US hospital industry	Calc: 375 million hrs x $63	$23.7 billion

As shown in Table 2, survey results provide an estimate of 5,040 total hours expended each month or 60,480 total hours each year by hospital personnel in IT, administration and clinical management. Using the 2019 AHA estimate of 6,210 registered U.S. hospitals, we compute 375.6 million hours for the entire industry each year. We also assume a fully loaded labor cost of $63 per hour. Multiplying total labor hours by the estimated labor rate, we compute a total industry impact of $23.7 billion dollars per annum.

In this research we define the four vendor risk management controls as follows:

Assessment of regulatory compliance: Conduct periodic assessments and monitor vendors to ensure compliance with contractually required security requirements, data protection and privacy regulations, especially HIPAA.

Enforcement of non-compliance with security requirements: Establish enforcement actions, termination penalties and remediation requirements for vendors that fail to achieve your organization's security requirements.

Data breach and cyber exploit incident response procedures: Establish procedures to respond to a data breach or cyber exploit caused by a vendor. These procedures can include formal documentation of incident response procedures, fire drills to practice response plans and the assignment of responsibility for communicating with customers, regulators, law enforcement and other key stakeholders.

Prioritization of vendor risks: Establish a risk prioritization process for the assessment and due diligence of vendors. Such a process could be based upon the type, value and business criticality of information assets your organization share with the vendor.

Organizations are not allocating sufficient budget to have an effective vendor risk management program. The average annual cybersecurity budget for organizations represented in this research is $12.05 million. Fifty-two percent of respondents say their organizations allocate an average of 17 percent of the cybersecurity budget or approximately $2 million for their vendor risk management programs. As shown below, respondents estimate it costs an average of $5 million to implement all four controls.

Table 1 presents the average cost to organizations that are fully or partially deploying each vendor-risk management control. Seventy-five percent of respondents say their organizations are either fully or partially deploying the enforcement of non-compliance with security requirements and this is the costliest control to implement. If an organization implements all four controls, the average annual cost can be almost $5 million.

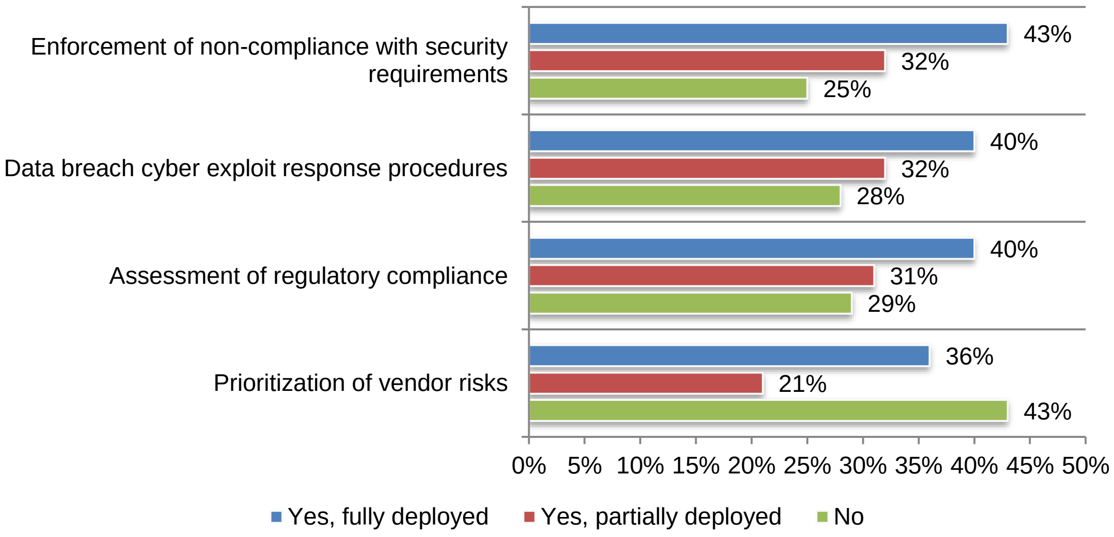
Table 1. Annual cost to implement vendor risk management control practices	**Extrapolated Cost**
Assessment of regulatory compliance	$1,240,950
Enforcement of non-compliance with security requirements	$1,351,750
Data breach cyber exploit response procedures	$1,186,300
Prioritization of vendor risks	$1,207,900
Total cost to implement vendor risk management practices	$4,986,900

Respondents were asked to estimate the annual cost if these controls were ineffective in preventing a data breach or cyberattack. The estimate is based on the total cost that results from a loss of reputation, brand damages, decline in revenue, downtime or the inability to recover from a disaster. The two most costly failures result from ineffective prioritization of vendor risks and data breach exploit response procedures.

Table 2. The annual cost if a data breach or cyberattack occurred due to the ineffectiveness of the control	**Extrapolated Cost**
Assessment of regulatory compliance	$4,129,250
Enforcement of non-compliance with security requirements	$4,653,750
Data breach cyber exploit response procedures	$5,178,250
Prioritization of vendor risks	$5,192,000

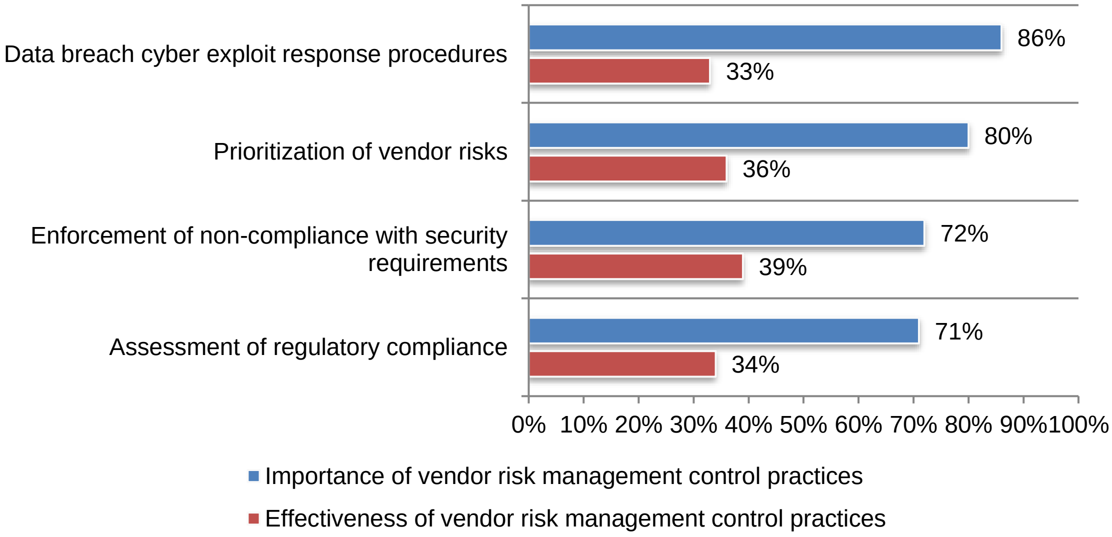
Vendor risk management controls practices are only partially deployed or not deployed at all. According to the findings, the majority of all data breaches experienced by the organizations in this research are caused by vendors. Figure 16 presents four control practices and the degree of deployment. As shown, 43 percent of respondents have not deployed the prioritization of vendor risks. Enforcement of non-compliance with security requirements is the control practice most often fully deployed.

Figure 16. Deployed vendor risk management control practices fully or partially deployed



Vendor management risk controls are considered important but not very effective. Figure 17 presents the importance and the effectiveness of the four vendor risk management practices. While 86 percent say data breach cyber exploit response procedures are very important, only 33 percent of respondents say the practice is very effective. While 80 percent say prioritization of vendor risks is considered very important, only 36 percent of respondents say it is very effective.

Figure 17. The importance and effectiveness of vendor risk management control practices
On a scale from 1 = Not important to 10 = Very important and 1 = Ineffective to 10 = Very effective,
7+ responses presented



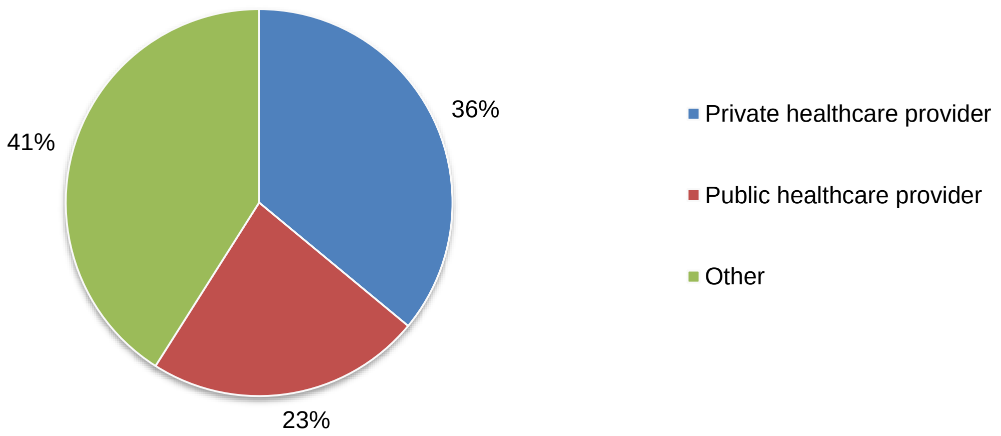
Part 3. Methods

The sampling frame is composed of 15,465 IT and IT security practitioners in healthcare companies who are involved in managing their organizations' vendor risk management programs. As shown in Table 3, 613 respondents completed the survey. Screening removed 59 surveys. The final sample was 554 surveys resulting in a 3.6 percent response rate.

Table 3. Sample response	**Freq**	**Pct%**
Total sampling frame	15,465	100.0%
Total returns	613	4.0%
Rejected or screened surveys	59	0.4%
Final sample	554	3.6%

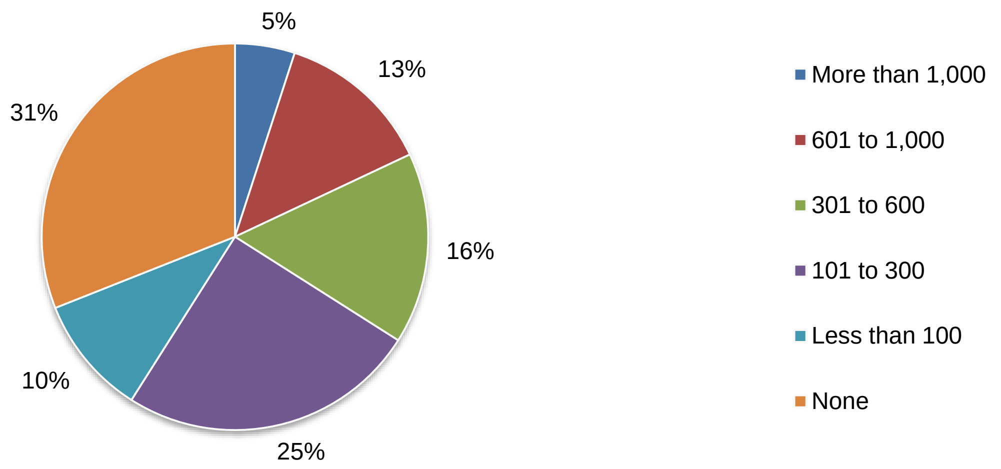
Thirty-six percent of respondents described their organization as a private healthcare provider and 23 percent of respondents described their organization as a public healthcare provider, as shown in Pie Chart 1

Pie Chart 1. Distribution by respondents' organization



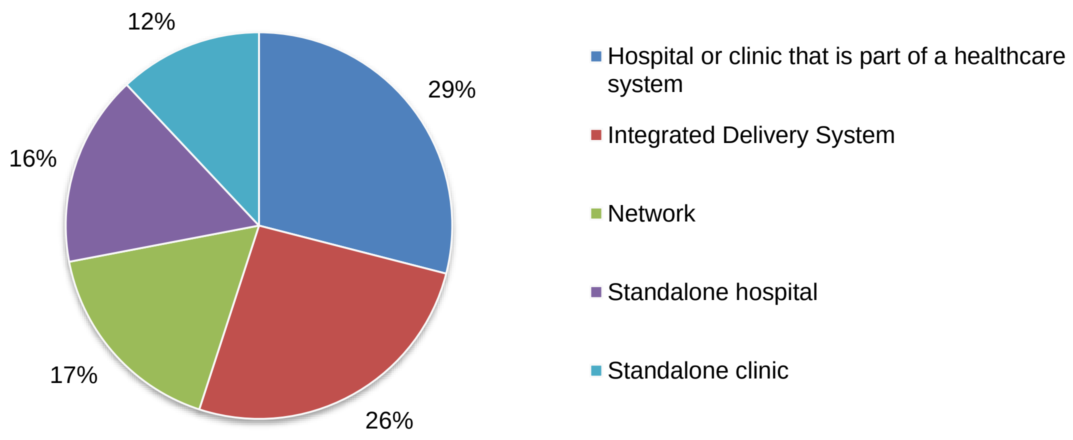
Pie chart 2 reveals that more than half (59 percent) of respondents reported their facility has more that 100 patient beds and 31 percent of respondents reported their facility does not have any patient beds.

Pie Chart 2. Distribution by facility size



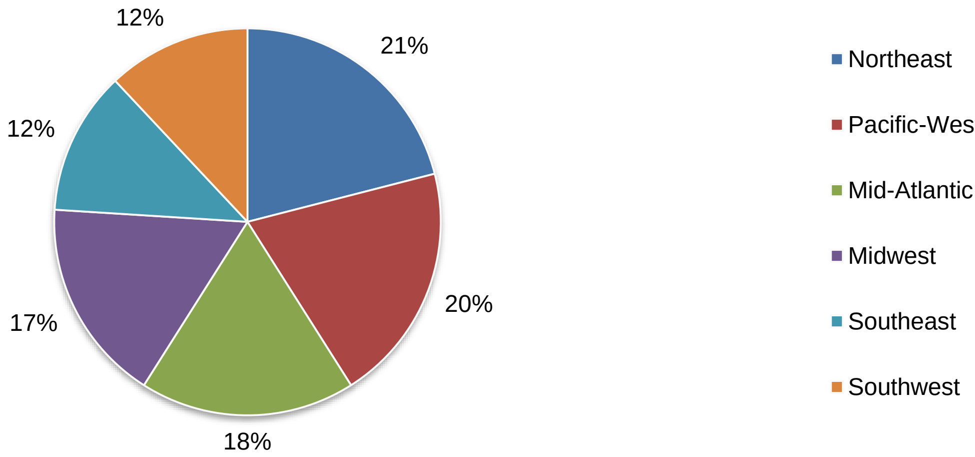
As shown in Pie Chart 3, twenty-nine percent of respondents reported their organizations' operating structure as a hospital or clinic. This is followed by 26 percent of respondents that described their operating structure as an integrated delivery system, network (17 percent of respondents), standalone hospital (16 percent of respondents) and a standalone clinic (12 percent of respondents).

Pie Chart 3. Distribution by operating structure



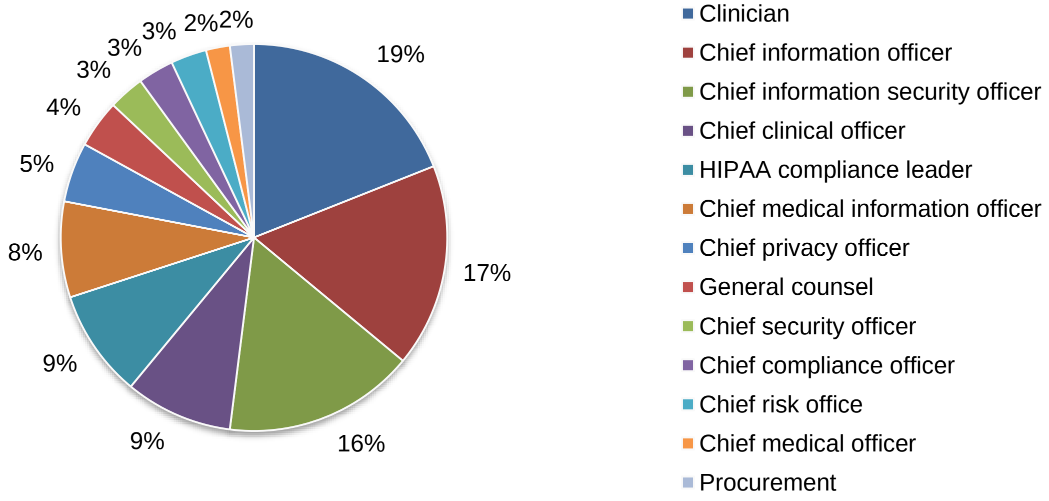
Pie Chart 4 reports the geographic location of respondents' organizations. Twenty-nine percent of respondents are located in the Northeast, followed by Pacific-West (20 percent of respondents), Mid-Atlantic (18 percent of respondents), Midwest (17 percent of respondents), Southeast (12 percent of respondents) and the Southwest (12 percent of respondents).

Pie Chart 4. Geographic location of respondents



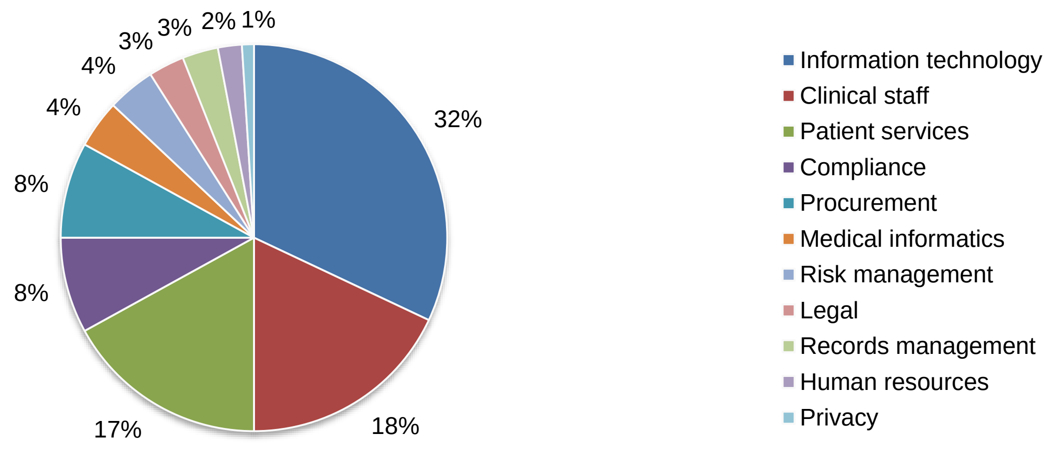
Pie Chart 5 reports the current role of the respondent or their supervisors' role. Nineteen percent of respondents reported their current role as clinician, 17 percent of respondents reported their current position as chief information officer and 16 percent of respondents reported their role as chief information security officer.

Pie Chart 5. Current role of the respondent or their supervisor



Pie Chart 6 reports the department or function of respondents. This chart identifies that 32 percent of respondents are located in information technology. This is followed by clinical staff (18 percent of respondents), and patient services (17 percent of respondents).

Pie Chart 6. Distribution of respondents by department or function



Part 4. Caveats to this study

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

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, 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 IT and IT security practitioners in healthcare companies who are involved in managing their organizations' vendor risk management programs. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

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

Appendix: Detailed Survey Results

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

Survey response	FY2019
Total sampling frame	15,465
Total returns	613
Rejected surveys	59
Final sample	554
Response rate	3.58%

Part 1. Screening Questions

S1. Is your organization a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act (HIPAA)?	FY2019
Yes	100%
No (stop)	0%
Total	100%

S2a. Does your healthcare company have a vendor risk management program (VRMP)?	FY2019
Yes	100%
No (stop)	0%
Total	100%

S3. What best describes your involvement in evaluating cyber and other risks of your third-party vendors?	FY2019
Evaluation of cyber risks	54%
Conduct assessments	60%
Review assessments and risk ratings	47%
Communicate risk to executive leadership	39%
Terminate relationships with third parties that do not meet our security and/or privacy requirements	50%
None of the above (stop)	0%
Total	250%

Part 2. Attributions: Strongly agree and Agree response combined	FY2019
Q1. Our organization is at risk for a data breach or serious security incident because we are unable to complete risk assessments of all our vendors.	54%
Q2. Current risk management processes using spreadsheets and emails are inefficient, not scalable, costly and do not reduce exposure to data breaches, ransomware and downtime.	76%
Q3. Moving to the cloud while connecting medical devices to the internet creates significant cyber risk exposure.	68%
Q4. Our organization reports on third-party vendor risk up to the Board.	34%
Q5. Our organization is required under HIPAA to annually assess the risk of our third-party vendors.	60%
Q6. Our organization assesses 100% of its vendors annually	27%
Q7. Investigations and fines from HHS and OCR for non-compliance due to deficiencies in vendor risk management is on the increase.	66%
Q8. Healthcare providers increasingly rely upon third-party medical devices which are connected to the internet and inherently risky.	72%
Q9. Third-party vendors account for the majority of all data breaches experienced by my organization over the past two years.	50%
Q10. Our current manual risk management processes cannot keep pace with the proliferation of digital applications and devices used in the healthcare ecosystem.	63%
Q11. Our current manual risk management processes cannot keep pace with the proliferation of cyber threats and vulnerabilities.	65%
Q12.Cybersecurity, privacy and regulatory requirements mandate that every healthcare provider identify, assess, monitor and mitigate risks caused by third-party vendor products or services.	58%
Q13. My organization saves time by automating inefficient risk management workflows that rely upon spreadsheets, emails and other manual processes.	44%
Q14. Time spent on vendor risk assessments takes resources away from high-value tasks, such as staff training, building controls over data assets, incident response planning, upstream communications and more.	60%
Q15. Senior executives/business owners are permitted go around or "shortcut" the third-party vendor risk assessment process if necessary to secure a lucrative business relationship.	59%

Part 3. Five features of automated risk management

Following are features of an automated vendor risk management platform for healthcare organizations. Please complete the questions using the 10-point scale provided below each feature.	
Standardization of vendor assessment questionnaire. Apply standardized questionnaires across multiple risk dimensions and product types in order to collect consistent results and compare them across the supply chain and industry. It is an efficient way to collect information from a large number of respondents. Statistical techniques can be used to determine validity, reliability, and statistical significance. The data forms the foundation for a predictive model.	
Q16a. How important is the standardization of a vendor assessment questionnaire to your organization's overall third-party vendor risk profile? From 1 = Not important to 10 = Very important	FY2019
1 to 2	6%
3 to 4	7%
5 to 6	13%
7 to 8	34%
9 to 10	40%
Total	100%
Extrapolated value	7.40

Q16b. What best defines your organization's ability to standardize its vendor assessment questionnaires today? From 1 = Low ability to 10 = High ability	FY2019
1 to 2	10%
3 to 4	18%
5 to 6	34%
7 to 8	23%
9 to 10	15%
Total	100%
Extrapolated value	5.80

Easy and immediate access to vendor assessments and supporting evidence. The ability to access a list of our current vendors with their assessment and risk rating.	
Q17a. How important is easy and immediate access to vendor risk assessments and other supporting evidence to your organization's cyber risk management profile? From 1 = Not important to 10 = Very important	FY2019
1 to 2	8%
3 to 4	7%
5 to 6	13%
7 to 8	30%
9 to 10	42%
Total	100%
Extrapolated value	7.32

Q17b. What best defines your organization’s ability to access vendor information in an easy and immediate basis today? From 1 = Low ability to 10 = High ability	FY2019
1 to 2	13%
3 to 4	21%
5 to 6	25%
7 to 8	21%
9 to 10	20%
Total	100%
Extrapolated value	5.78

Real-time risk alerts and notifications. The ability to continuously update changes to a third-parties risk based on vulnerabilities, patches, minor and major product releases, and end-of-life notices.

Q18a. How important are real-time risk alerts and notifications to your organization’s third-party risk management process? From 1 = Not important to 10 = Very important	FY2019
1 to 2	6%
3 to 4	8%
5 to 6	8%
7 to 8	33%
9 to 10	45%
Total	100%
Extrapolated value	7.56

Q18b. What best defines your organization’s ability to effectively capture and act upon real-time third-party risk alerts and notifications today? From 1 = Low ability to 10 = High ability	FY2019
1 to 2	20%
3 to 4	21%
5 to 6	21%
7 to 8	25%
9 to 10	13%
Total	100%
Extrapolated value	5.30

Part 4. Vendor risk management control practices

Assessment of regulatory compliance: Conduct periodic assessments and monitor vendors to ensure compliance with contractually required security requirements and data protection and privacy regulations (especially HIPAA).

Q19a. Does your organization deploy this vendor-related control or practice?	FY2019
Yes, fully deployed	40%
Yes, partially deployed	31%
No	29%
Total	100%

Q19b. If yes, how important is this control at moderating or mitigating a vendor-related data breach or other high-risk security incident? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	FY2019
1 to 2	8%
3 to 4	9%
5 to 6	12%
7 to 8	25%
9 to 10	46%
Total	100%
Extrapolated value	7.34

Q19c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this vendor-related control or practice.	FY2019
Less than $10,000	10%
$10,000 to $50,000	14%
$50,001 to $100,000	3%
$100,001 to $1,000,000	28%
$1,000,001 to $5,000,000	18%
$5,000,001 to $10,000,000	5%
More than $10,000,000	2%
Total	80%
Extrapolated value	$1,240,950

Q19d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a vendor-related cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	FY2019
1 to 2	21%
3 to 4	24%
5 to 6	21%
7 to 8	13%
9 to 10	21%
Total	100%
Extrapolated value	5.28

Q19e. Please provide your best estimate for the annual cost incurred by your organization if it failed to implement the above-mentioned control over vendors at a high level of effectiveness and this resulted in a material data breach or successful cyberattack. In your estimate, please consider costs such as reputation impact, brand damages, decline in revenue, downtime or the inability to recover from a disaster such as an earthquake	FY2019
Less than $10,000	4%
$10,000 to $50,000	6%
$50,001 to $100,000	11%
$100,001 to $1,000,000	18%
$1,000,001 to $5,000,000	16%
$5,000,001 to $10,000,000	31%
More than $10,000,000	14%
Total	100%
Extrapolated value	$ 4,129,250

Enforcement of non-compliance with your organization's security requirements: Establish enforcement actions, termination penalties and remediation requirements for vendors that fail to achieve your organization's objective security requirements.

Q20a. Does your organization deploy this vendor-related control or practice?	FY2019
Yes, fully deployed	43%
Yes, partially deployed	32%
No	25%
Total	100%

Q20b. If yes, how important is this control at moderating or mitigating a vendor-related data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	FY2019
1 to 2	7%
3 to 4	8%
5 to 6	13%
7 to 8	25%
9 to 10	47%
Total	100%
Extrapolated value	7.44

Q20c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this vendor-related control.	FY2019
Less than $10,000	8%
$10,000 to $50,000	12%
$50,001 to $100,000	21%
$100,001 to $1,000,000	24%
$1,000,001 to $5,000,000	30%
$5,000,001 to $10,000,000	5%
More than $10,000,000	0%
Total	100%

Extrapolated value	$ 1,351,750

Q20d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a vendor-related cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	FY2019
1 to 2	14%
3 to 4	26%
5 to 6	21%
7 to 8	23%
9 to 10	16%
Total	100%
Extrapolated value	5.52

Q20e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control over vendors at a high level of effectiveness and this resulted in a material data breach or successful cyberattack. In your estimate, please consider costs such as reputation impact, brand damages, decline in revenue, downtime or the inability to recover from a disaster such as an earthquake	FY2019
Less than $10,000	0%
$10,000 to $50,000	0%
$50,001 to $100,000	11%
$100,001 to $1,000,000	21%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	23%
More than $10,000,000	20%
Total	100%
Extrapolated value	$ 4,653,750

Data breach and cyber exploit incident response procedures: Establish procedures to respond to a data breach or cyber exploit caused by one of your organization's vendors. These procedures can include formal documentation of incident response procedures, fire drills to practice response plans and the assignment of responsibility for communicating with customers, regulators, law enforcement and other key stakeholders.

Q21a. Does your organization deploy this vendor-related control or practice?	FY2019
Yes, fully deployed	40%
Yes, partially deployed	32%
No	28%
Total	100%

Q21b. If yes, how important is this control at moderating or mitigating a vendor-related data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	FY2019
1 to 2	0%
3 to 4	2%
5 to 6	12%
7 to 8	42%
9 to 10	44%
Total	100%
Extrapolated value	8.06

Q21c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this vendor-related control.	FY2019
Less than $10,000	6%
$10,000 to $50,000	15%
$50,001 to $100,000	28%
$100,001 to $1,000,000	31%
$1,000,001 to $5,000,000	13%
$5,000,001 to $10,000,000	4%
More than $10,000,000	3%
Total	100%
Extrapolated value	$ 1,186,300

Q21d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a vendor-related cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	FY2019
1 to 2	20%
3 to 4	22%
5 to 6	25%
7 to 8	17%
9 to 10	16%
Total	100%
Extrapolated value	5.24

Q21e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control over vendors at a high level of effectiveness and this resulted in a material data breach or successful cyberattack. .In your estimate, please consider costs such as reputation impact, brand damages, decline in revenue, downtime or the inability to recover from a disaster such as an earthquake.	FY2019
Less than $10,000	0%
$10,000 to $50,000	0%
$50,001 to $100,000	5%
$100,001 to $1,000,000	19%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	30%
More than $10,000,000	21%
Total	100%
Extrapolated value	$5,178,250

Prioritization of vendor risks: Establish a risk prioritization process for the assessment and due diligence of vendors. Such a process could be based upon the type, value and business criticality of information assets your organization shares with the vendor.

Q22a. Does your organization deploy this vendor-related control or practice?	FY2019
Yes, fully deployed	36%
Yes, partially deployed	21%
No	43%
Total	100%

Q22b. If yes, how important is this control at moderating or mitigating a vendor-related data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	FY2019
1 to 2	3%
3 to 4	6%
5 to 6	11%
7 to 8	34%
9 to 10	46%
Total	100%
Extrapolated value	7.78

Q22c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this vendor-related control.	FY2019
Less than $10,000	5%
$10,000 to $50,000	18%
$50,001 to $100,000	23%
$100,001 to $1,000,000	30%
$1,000,001 to $5,000,000	18%
$5,000,001 to $10,000,000	4%
More than $10,000,000	2%
Total	100%
Extrapolated value	$1,207,900

Q22d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a vendor-related cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	FY2019
1 to 2	20%
3 to 4	21%
5 to 6	23%
7 to 8	21%
9 to 10	15%
Total	100%
Extrapolated value	5.30

Q22e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control over vendors at a high level of effectiveness and this resulted in a material data breach or successful cyberattack. In your estimate, please consider costs such as reputation impact, brand damages, decline in revenue, downtime or the inability to recover from a disaster such as an earthquake.	FY2019
Less than $10,000	0%
$10,000 to $50,000	0%
$50,001 to $100,000	2%
$100,001 to $1,000,000	11%
$1,000,001 to $5,000,000	29%
$5,000,001 to $10,000,000	45%
More than $10,000,000	13%
Total	100%
Extrapolated value	$5,192,000

Part 5. General Questions

Q23. Approximately, how many vendors does your organization have under contract and manage today?	FY2019
Less than 100	7%
100 to 500	17%
501 to 1,000	28%
1,001 to 2,000	27%
2,001 to 3,000	13%
3,001 to 4,000	5%
4,001 to 5,000	2%
More than 5,000	1%
Total	100%
Extrapolated value	1,320

Q24a. Do some of your organization's vendors receive a more comprehensive assessment or level of due diligence than others?	FY2019
Yes	64%
No, all vendors receive the same level of due diligence	36%
Total	100%

Q24b. If yes, how do you determine which vendors to prioritize for due diligence and assessment? Please select your top three by priority.	FY2019
The vendor is critical to our organization's ability to meet its business objectives and obligations	65%
The vendor has access to our most sensitive and confidential information	50%
The vendor has the potential to affect our organization's ability to comply with regulations	49%
The vendor has access to PHI	71%
The vendor assists in the delivery of patient care	63%
Other	2%
Total	300%

Q24c. Which vendor types represent the highest potential risk based on impact to patient care. Please select your top four by priority.	FY2019
Clinical researchers	47%
Business consultants	33%
Cloud providers	53%
Payroll providers	17%
Outsourced HR	19%
Outsourced IT	32%
Application developers	41%
Payment processors	19%
Outsourced or co-located data centers	20%
Clinical applications	56%
Back-office applications	20%
Affiliated practices	8%
Medical device manufacturers	31%
Other	4%
Total	400%

Q24d. What actions does your organization take if a vendor has gaps in its security controls or practices that could put your organization at risk?	FY2019
Relationship is terminated	28%
Mitigation or remediation is requested	33%
Collaborate with third party to improve its security measures	27%
Risk is transferred using insurance	12%
Other	0%
Total	100%

Part 6. Data breaches

Q25a. Has your organization experienced one or more data breaches caused by an insecure vendor over the past 2 years?	FY2019
Yes	56%
No	38%
Unsure	6%
Total	100%

Q25b. If yes, how many separate data breach incidents did your organization experience?	FY2019
One	40%
2 to 3	43%
4 to 5	13%
More than 5	4%
Total	100%
Extrapolated value	2.30

Q25c. If yes, how many records were lost or stolen as a result of all vendor-related data breaches experienced over the **past two years**?	FY2019
Less than 100	9%
100 to 1,000	14%
1,001 to 5,000	21%
5,001 to 10,000	38%
10,001 to 50,000	16%
50,001 to 1,000,000	2%
1,000,001 to 5,000,000	0%
More than 5,000,000	0%
Total	100%
Extrapolated value	5,542

Q25d. If yes, please provide your best estimate for the total cost of all vendor-related data breaches experienced by your organization over **the past 2 years?**	FY2019
Less than $10,000	8%
$10,000 to $50,000	17%
$50,001 to $100,000	23%
$100,001 to $1,000,000	20%
$1,000,001 to $5,000,000	13%
$5,000,001 to $10,000,000	15%
$10,000,001 to $50,000,000	3%
More than $50,000,000	1%
Total	100%
Extrapolated value	$2,922,750

Q25e. Please provide your best estimate for the likelihood (probability) of a vendor-related data breach involving 10,000 or more records containing sensitive or confidential information over **the next two years**?	FY2019
Less than 1%	1%
1% to 5%	5%
6% to 10%	11%
11% to 20%	13%
21% to 30%	30%
31% to 40%	21%
41% to 50%	13%
More than 50%	6%
Total	100%
Extrapolated value	27.3%

Q26. How important is the process for performing risk assessments of your organization’s vendors? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	FY2019
1 to 2	2%
3 to 4	3%
5 to 6	9%
7 to 8	39%
9 to 10	47%
Total	100%
Extrapolated value	8.02

Q27. What is the total cost incurred by your organization to complete all required risk assessments on an annual basis.	FY2019
Less than $50,000	5%
$50,000 to $100,000	21%
$100,001 to $500,000	24%
$500,001 to $1,000,000	18%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	5%
$10,000,001 to 50,000,000	2%
$50,000,001 to $100,000,000	4%
More than $100,000,000	0%
Total	100%
Extrapolated value	$4,829,000

Q28. How effective or accurate are risk assessments at reflecting your vendors’ risk profile? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	FY2019
1 to 2	13%
3 to 4	21%
5 to 6	30%
7 to 8	20%
9 to 10	16%
Total	100%
Extrapolated value	5.60

Q29. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to perform vendor assessments at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in revenue, etc.	FY2019
Less than $50,000	0%
$50,000 to $100,000	6%
$100,001 to $500,000	12%
$500,001 to $1,000,000	17%
$1,000,001 to $5,000,000	18%
$5,000,001 to $10,000,000	24%
$10,000,001 to 50,000,000	12%
$50,000,001 to $100,000,000	6%
More than $100,000,000	5%
Total	100%
Extrapolated value	$16,608,000

Part 7. Vendor risk assessment

Q30. What percentage of vendors are assessed to ensure they meet your organization’s security and/or privacy requirements?	FY2019
Less than 25%	30%
25% to 50%	37%
51% to 75%	22%
76% to 100%	11%
Total	100%
Extrapolated value	41%

Q31. How frequently are vendors assessed?	FY2019
Real-time	5%
Monthly	13%
Quarterly	11%
Annually	30%
On-demand	18%
No regular schedule	23%
Total	100%

Q32. How important is understanding the potential financial risk of vendors?	FY2019
1 to 2	2%
3 to 4	3%
5 to 6	8%
7 to 8	42%
9 to 10	45%
Total	100%
Extrapolated value	8.00

Q33. How important is understanding the information security risk of vendors?	FY2019
1 to 2	1%
3 to 4	5%
5 to 6	12%
7 to 8	37%
9 to 10	45%
Total	100%
Extrapolated value	7.90

Q34. How important is understanding the availability risk of vendors?	FY2019
1 to 2	0%
3 to 4	11%
5 to 6	13%
7 to 8	35%
9 to 10	41%
Total	100%
Extrapolated value	7.62

Q35. How important is understanding the resiliency of vendors?	FY2019
1 to 2	0%
3 to 4	12%
5 to 6	12%
7 to 8	33%
9 to 10	43%
Total	100%
Extrapolated value	7.64

Q36. How important is understanding the potential legal and regulatory risk of vendors?	FY2019
1 to 2	0%
3 to 4	3%
5 to 6	12%
7 to 8	41%
9 to 10	44%
Total	100%
Extrapolated value	8.02

\

Q37. What tools does your organization use to assess vendor risk? Please select only one choice.	FY2019
Mostly manual procedures (i.e. spreadsheets)	31%
Mostly automated procedures and tools	33%
A combination of automated and manual procedures and tools	35%
Other	1%
Total	100%

Q38. On average, how much time (hours) is spent monthly completing vendor risk assessments of your organization?	FY2019
Less than 100 hours	4%
100 to 500 hours	11%
501 hours to 1,000 hours	28%
1,001 to 5,000 hours	29%
5,001 to 10,000 hours	16%
10,001 to 25,000 hours	7%
More than 25,000 hours	5%
Total	100%
Extrapolated value	5,040

Q39. On average, how many FTEs are dedicated to completing vendor risk assessments	FY2019
None	4%
1 to 2	33%
3 to 4	46%
5 to 6	11%
7 to 8	5%
9 to 10	0%
More than 10	1%
Total	100%
Extrapolated average	3.21

Q40. As part of your organization’s vendor risk management process, what percent of third-party assessments result in disqualification prior to doing business with them?	FY2019
Less than 1%	11%
1% to 5%	21%
6% to 10%	31%
11% to 20%	18%
21% to 30%	13%
31% to 40%	6%
41% to 50%	0%
More than 50%	0%
Total	100%
Extrapolated value	11%

Q41. As part of your organization’s vendor risk management process, what percent of third-party assessments result in a requirement to remediate prior to doing business with them?	FY2019
Less than 1%	8%
1% to 5%	10%
6% to 10%	15%
11% to 20%	19%
21% to 30%	15%
31% to 40%	24%
41% to 50%	7%
More than 50%	2%
Total	100%
Extrapolated value	21%

Q42. How valuable are the results of vendor risk assessments performed by your organization? In the context of this survey, please define value as cost savings and/or risk reduction resulting from a well-functioning vendor risk assessment process or program.	FY2019
Very valuable, the results provide our organization with actionable insights that can be reported to the C-suite and board of directors	40%
Somewhat valuable, the results provide information on what actions our organization should take	42%
Not valuable, the results do not provide any insights	18%
Total	100%

Q43. Which business function realizes the greatest benefit as a result of a well-functioning vendor risk assessment process or program? Please select your top four choices.	FY2019
Board of directors	8%
CEO/COO	31%
CIO	23%
CTO	8%
CISO/CSO	26%
CFO/ finance	26%
Legal (OGC)	45%
Compliance	59%
Procurement/purchasing	61%
Clinical departments	75%
Risk management	34%
Other	4%
Total	400%

Part 8. Budget questions

Q44. Approximately, what is the dollar range that best describes your organization’s **cybersecurity budget for 2019**?	FY2019
< $1 million	5%
$1 to 5 million	10%
$6 to $10 million	25%
$11 to $15 million	33%
$16 to $20 million	22%
$21 to $25 million	3%
$26 to $50 million	2%
> $50 million	0%
Total	100%
Extrapolated value	$12.05

Q45a. Does your organization budget (earmark) funds to support its vendor risk management program?	FY2019
Yes	52%
No	47%
Unsure	1%
Total	100%

Q45b. If yes, what percentage of the cybersecurity budget is allocated to support its vendor risk management program?	FY2019
Less than 10%	18%
10% to 15%	27%
16% to 20%	28%
21% to 30%	22%
31% to 40%	4%
41% to 50%	1%
More than 50%	0%
Total	100%
Extrapolated value	17%

Q45c. If yes, who “owns” or approves purchases against the vendor risk management budget within your organization? Please select one best choice.	FY2019
CEO/COO	4%
CIO	10%
CTO	1%
CISO/CSO	10%
CFO/ finance	5%
Legal (OGC)	25%
Compliance	21%
Procurement/purchasing	6%
Clinical departments	13%
Risk management	5%
Other	0%
Total	100%

Part 5: Organizational characteristics

Please select the category that best describes your role and your healthcare organization.	
D1. What best describes your organization?	FY2019
Public healthcare provider	23%
Private healthcare provider	36%
Other	41%
Total	100%

D2. How many patient beds (capacity) does your entire healthcare facility or health system have?	FY2019
None	31%
Less than 100	10%
101 to 300	25%
301 to 600	16%
601 to 1,000	13%
More than 1,000	5%
Total	100%

D3. [Excluding D2 = None] What best describes its operating structure?	FY2019
Integrated Delivery System	26%
Hospital or clinic that is part of a healthcare	29%
Network	17%
Standalone hospital	16%
Standalone clinic	12%
Other	0%
Total	100%

D4. Please indicate the region of the United States where you are located.	FY2019
Northeast	21%
Mid-Atlantic	18%
Midwest	17%
Southeast	12%
Southwest	12%
Pacific-West	20%
Total	100%

D5. What best describes your role or the role of your supervisor?	FY2019
Chief security officer	3%
Chief information security officer	16%
Chief information officer	17%
Chief privacy officer	5%
Chief compliance officer	3%
Chief medical officer	2%
Chief clinical officer	9%
Chief risk office	3%
Chief medical information officer	8%
Procurement	2%
Chief development officer	0%
General counsel	4%
HIPAA compliance leader	9%
Clinician	19%
Other	0%
Total	100%

D6. What best describes the department or function where you are located?	FY2019
Compliance	8%
Privacy	1%
Information technology (IT)	32%
Legal	3%
Procurement	8%
Marketing	0%
Medical informatics	4%
Clinical staff	18%
Patient services	17%
Records management	3%
Risk management	4%
Development – foundation	0%
Planning	0%
Human resources	2%
Other	0%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call 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.

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.