Ponemon INSTITUTE

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

Sponsored by Censinet

Independently conducted by Ponemon Institute LLC

Publication Date: September 2021

Ponemon INSTITUTE

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

Prepared by Ponemon Institute, September 2021

Executive Summary

The purpose of this research is to understand how COVID-19 has impacted how healthcare delivery organizations protect patient care and patient information from increasing virulent cyberattacks, especially ransomware. Prior to COVID-19, 55 percent of respondents say they were **not** confident they could mitigate the risks of ransomware. In the age of COVID-19, 61 percent of respondents are **not** confident or have no confidence.

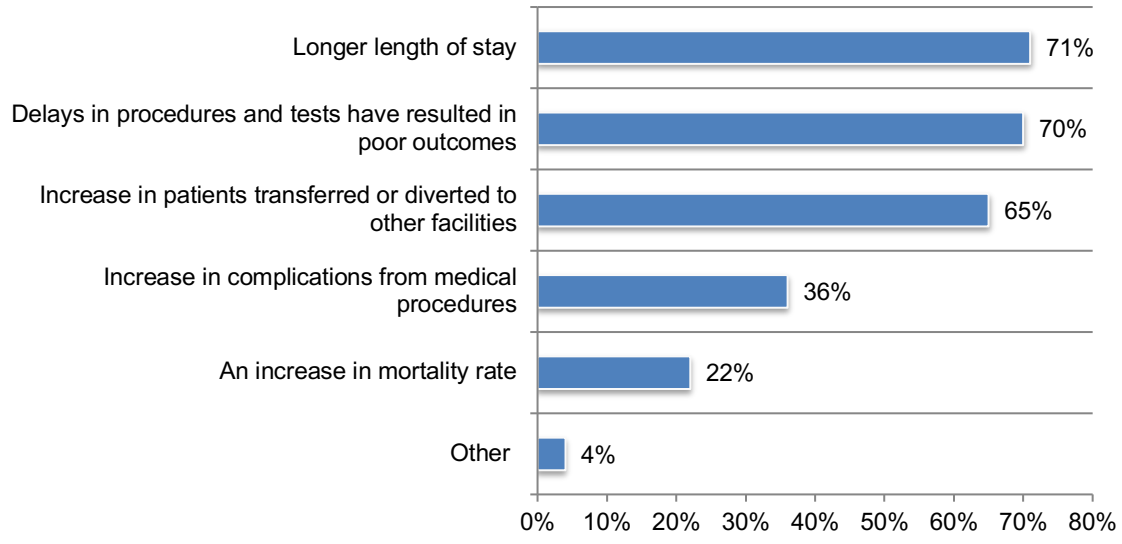
Sponsored by Censinet, Ponemon Institute surveyed 597 IT and IT security professionals in Healthcare Delivery Organizations (HDOs). In the context of this research, HDOs are entities that deliver clinical care and rely upon the security of third parties with whom they contract services and products. These include integrated delivery networks, regional health systems, community hospitals, physician groups, and payers.

Ransomware attacks on healthcare organizations can be a life-or-death situation.
The onset of COVID-19 introduced new risk factors to HDOs, including remote work, new systems to support it, staffing challenges, and elevated patient care requirements. There's been a great deal of media coverage on the rise of cyberattacks such as ransomware both within the healthcare industry and beyond. This research focuses on the healthcare industry to understand the extent to which HDOs are being targeted and ascertain the impact of those attacks. Both are covered in-depth in the key findings section of the report.

Over the last two years, 43 percent of respondents say their HDOs experienced a ransomware attack. Of these respondents, 67 percent of respondents say their HDO had one and 33 percent of respondents say they experienced two or more.

As shown in Figure 1, these attacks risk patient safety, data, and overall care availability. Respondents report that ransomware attacks had a significant impact on patient care, reporting longer length of stay (71 percent of respondents), delays in procedures and tests (70 percent of respondents), increase in patient transfers or facility diversions (65 percent of respondents) and an increase in complications from medical procedures (36%) and mortality rates (22%).

Figure 1. What impact does ransomware have on patient care?
More than one response from the 43 percent of respondents in HDOs that had a ransomware attack.



HDOs forecast that the number of contracted third parties will increase by 30 percent over the next 12 months

Driven by cost containment, regulatory directives and the demand for accessible, higher-quality patient care, HDOs have shifted to the digitization and distribution of health information. Moreover, medical devices, whether in patient rooms or labs, rely on network connectivity for operations and maintenance.

Nearly all of the technology components described are not developed by the HDO. These include software, services, and hardware development from organizations known as **third parties**. This study revealed that the average number of third parties that organizations contract with is 1,950, and this will increase to an average of 2,541 in the next 12 months.

Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third party such as secure operating systems and other software in medical devices. Other risks involve how the HDOs deploy and use third parties, including storing protected health information (PHI) on cloud-based systems that weren't meant to support it. In either case, the risk created by the third party or the HDO use of the third party needs to be managed. The burden is on the HDO to perform assessments throughout their relationship with the third party (e.g., procurement, implementation, usage, updates, termination, etc.).

Third-Party Risk Management is Hard, and COVID-19 Made it Worse

This research also looks at the capabilities and maturity of HDOs to manage third-party risk, both before and during COVID-19. According to only 44 percent of respondents, controls critical to assessing third-party risks are only partially accomplished in HDOs. Only 40 percent of respondents say their organization always completes a risk assessment of its third parties prior to contracting with them. However, 38 percent of respondents state the assessment findings are ignored by leaders.

Re-assessments are another critical part of third-party risk management and are not conducted as often as required. More than half (53 percent) of respondents say re-assessments are conducted only on-demand or on no regular schedule.

Recommendations for Mitigating Ransomware and Third-Party Risks

According to the findings, healthcare organizations are less prepared to deal with third-party risks. Following are recommended steps for HDOs to take to protect patient safety, data, and care operations.

- Invest in workflow automation, resources, and processes to establish a digital inventory of all third parties and PHI records. An HDO must know the number and location of PHI records that are accessed, transmitted or stored by third-party products or services.

- Increase overall risk coverage of third parties by leveraging automation to conduct more assessments. The average number of third parties that organizations contract with is expected to increase from 1,950 to 2,541 over the next 12 months. However, only 40 percent of respondents say their organizations always complete a risk assessment prior to engaging with a third party. If their organizations conduct an assessment, only 38 percent of respondents say their leaders always accept their recommendation not to contract with them.

- Allocate resources and funding to re-assess high-risk third parties. Currently, only an average of 32 percent of critical and high-risk third parties are assessed annually, and only an average of 27 percent of these third parties are re-assessed annually.

- Increase efforts to secure medical devices. Only 36 percent of respondents say their organizations know where all medical devices are. Only 35 percent of respondents say they know when a medical device vendor's operating device is end-of-life or out-of-date. Only 29 percent of respondents say they know the non-planned expense of medical device operating system patches.

- Ensure critical steps for identifying and mitigating third-party risks are in place. Sixty percent of organizations represented in this research had a data breach in the past two years, resulting in an average of 28,505 records containing sensitive and confidential information compromised. According to the research, organizations can only partially evaluate the various threats targeting their assets and IT vulnerabilities. They also lack the capability to continuously monitor vendor risks.

- Assign risk accountability and ownership to one role. The ability to execute an enterprise-wide risk management strategy is affected by not assigning accountability and ownership to one role.

Part 1. Key findings

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

- Effectiveness in managing the threats created by third parties
- Third-party vendor risk management programs and relationships
- Impact of cyberattacks such as ransomware on patient care

In the context of this research, third parties and vendors are used interchangeably. Third party or vendor risk management is the application of rigorous and systematic analytic techniques to the evaluation of organizational, product and/or services risks that impact the HDO enterprise, including information assets and IT infrastructure. Cyber risk management is considered a component of vendor risk management.

Effectiveness in managing the threats created by high-risk third parties

Controls critical to assessing third-party risks are only partially accomplished. Figure 2 lists four steps organizations have taken to assess and prioritize vendor risks respondents and if they are partially or fully accomplished to assess and prioritize vendor risks.

The step most often fully accomplished is identifying controls at the various layers to ensure all risks are at a level acceptable to the business. However, only 44 percent of organizations represented in this research have fully accomplished this step. Twenty-two percent of respondents say their organizations have either not accomplished (13 percent) or not attempted (9 percent).

This is followed by identifying key information needed to assess third-party risks. Only 35 percent of respondents have fully accomplished this step and only 25 percent of respondents say continuous monitoring of vendor risks is fully accomplished. Fifty percent of respondents say this step has not been accomplished (27 percent) or not attempted (23 percent).

Figure 2. Steps taken to assess and prioritize third-party risks

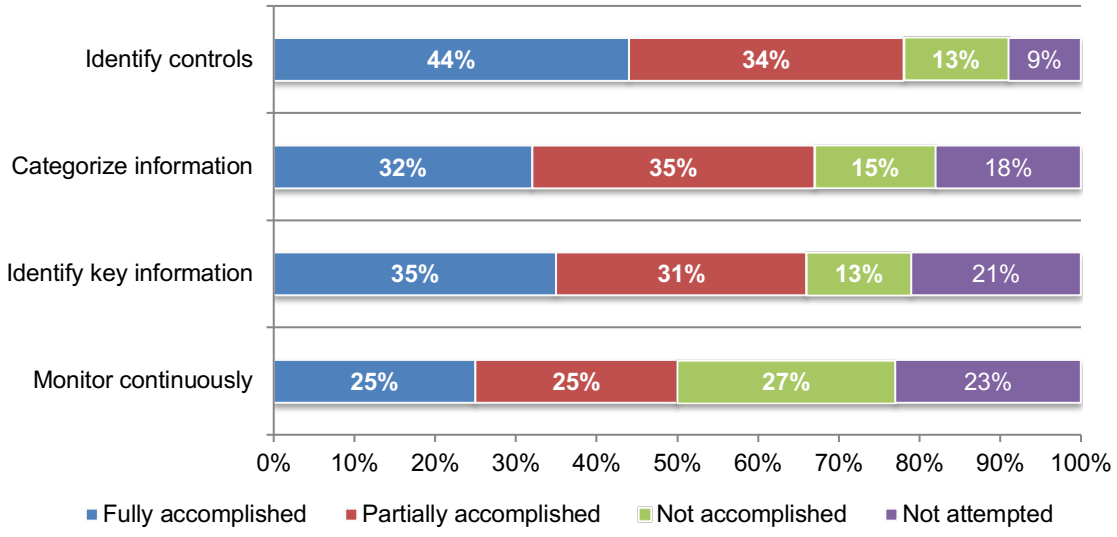
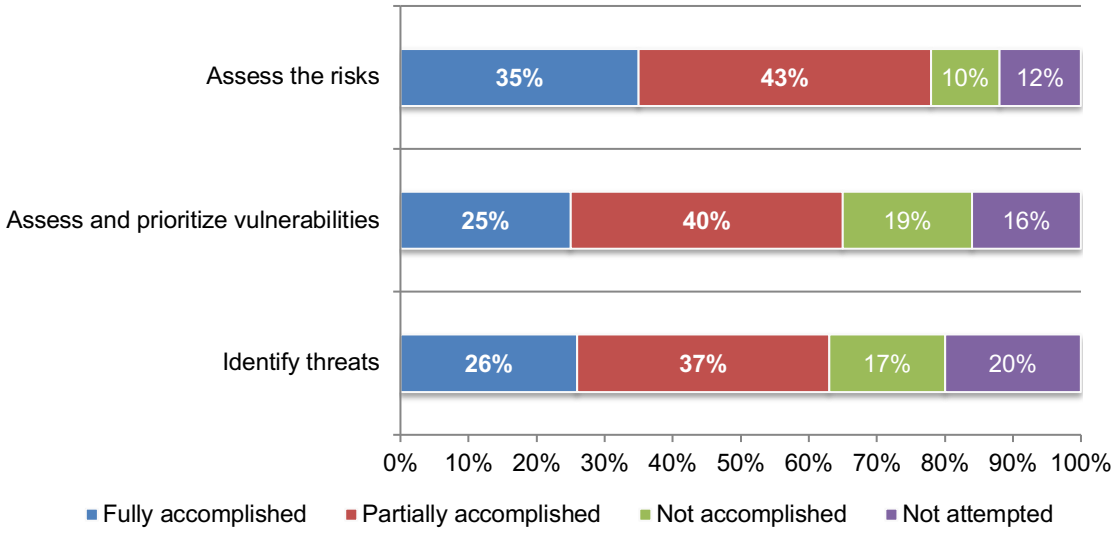


Figure 3 presents the status of three steps taken to assess the risks, prioritize vulnerabilities and identify threats. The most often fully accomplished step is assessing the risks posed against the organization determined by examining the various threats, the source of threats, the likelihood a threat will materialize and the impact a threat will have on protected information (35 percent of respondents).

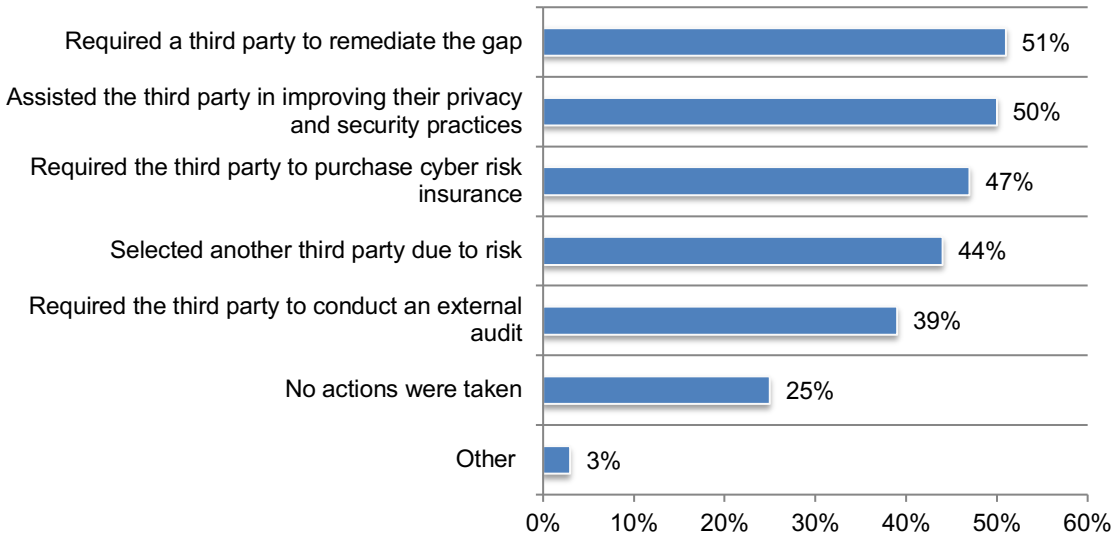
Only 25 percent of respondents say their organizations have fully accomplished the step to assess and prioritize vulnerabilities in existing controls and ascertain the likelihood that they will be exploited and what the potential impact of an incident will be. Only 26 percent of respondents say their organizations fully accomplished the step to evaluate the variety and source of threats targeting the organization and its assets and vulnerabilities.

Figure 3. Steps taken to identify threats, assess risks, and prioritize vulnerabilities



Once gaps in a third party's privacy and security practices and policies were discovered, only 44 percent of respondents say their organizations selected another third party due to risk. According to Figure 4, once these gaps were identified, 51 percent of respondents say their organizations required a third party to remediate the gap, and 50 percent of respondents say they assisted the third party in improving their privacy and security practices.

Figure 4. Did your organization take any of the following actions when gaps in a third-party's privacy and security practices and policies were discovered?
More than one response permitted

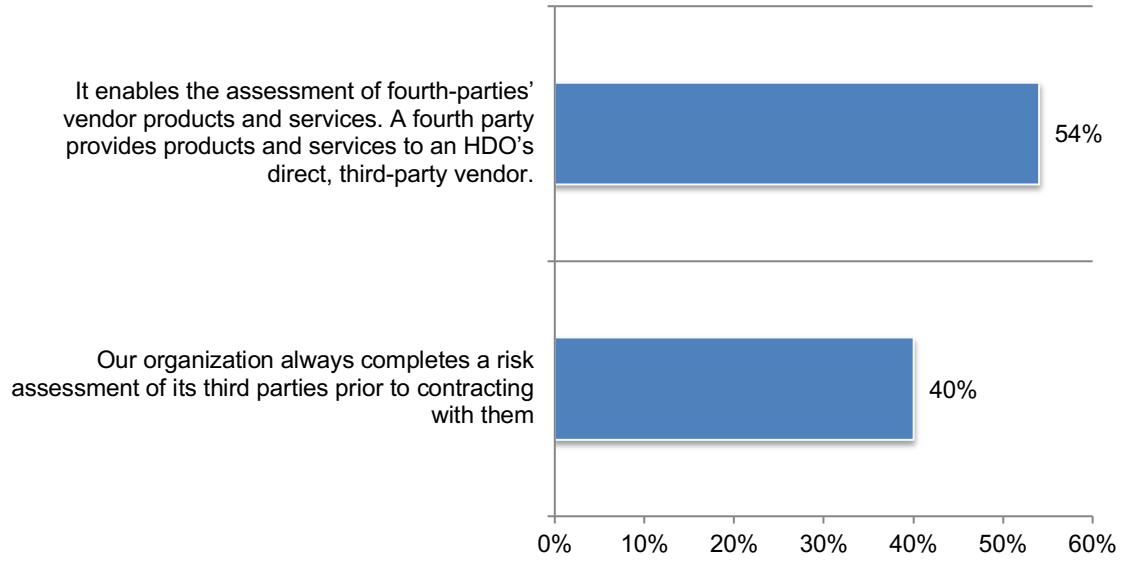


Organizations will contract with more third parties in the next 12 months, intensifying the need to identify those high-risk vendors and third parties. Currently, the average number of third parties that organizations contract with is 1,950, and this will increase to an average of 2,541 in the next 12 months. An average of 43 percent of the 1,950 third parties have access to these organizations' PHI, and an average of approximately 1,276 have been assessed.

According to Figure 5, 54 percent of respondents say their organizations' vendor risk management program includes having third parties assess fourth parties' vendor products and services that are provided to them. In the context of this research, a fourth party provides products and services to an HDO's direct third-party vendor.

Only 40 percent of respondents say their organization always completes a risk assessment of its third parties **prior to contracting with them**. If their organizations assess a third party prior to contracting them and find they are a high risk, only 38 percent of respondents say their organizations' leaders always accept their recommendation not to contract with them.

Figure 5. The capabilities of vendor risk programs
Strongly agree and Agree responses combined

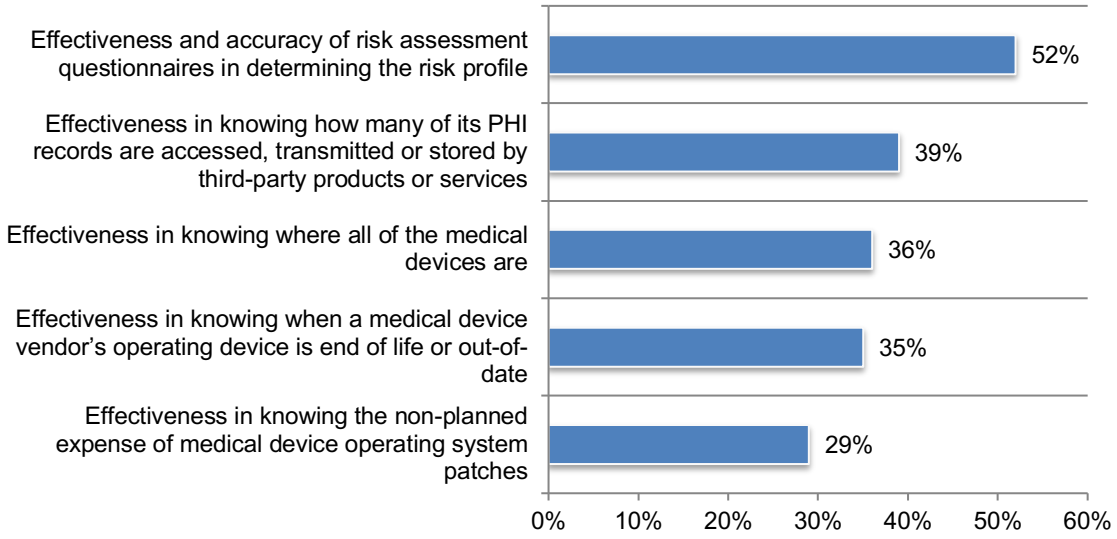


Healthcare organizations are at risk because they do not know how many of their PHI records are accessed, transmitted, or stored by third-party products or services. Respondents were asked to rate the effectiveness of their organizations' ability to reduce healthcare risks on a scale of 1 = ineffective to 10 = very effective. Figure 6 shows the high and highly effective responses (7+ responses). While more than half of respondents (52 percent) say their organizations are effective in having accurate risk assessment questionnaires that determine the risk profile, only 39 percent of respondents know how many of their organizations' PHI records are accessed, transmitted, or stored by third-party products or services.

The insecurity of medical devices can have an adverse impact on patient care, as shown in Figure 6. Respondents were also asked to rate the effectiveness of ensuring the security of their medical devices.

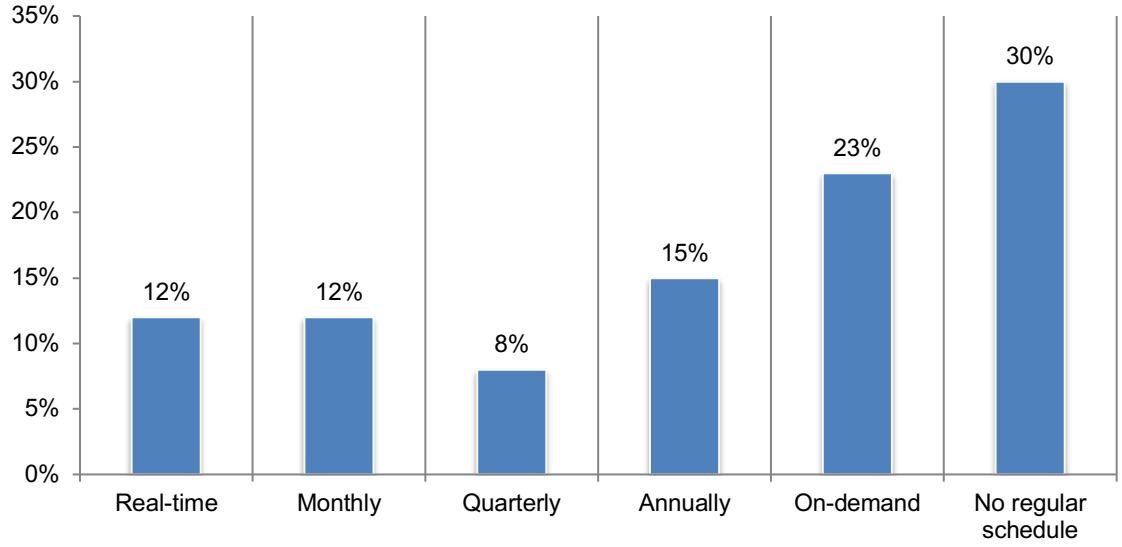
Only 36 percent of respondents say their organizations are effective in knowing where all medical devices are, 35 percent of respondents say they know when a medical device vendor's operating device is end-of-life or out-of-date and 29 percent of respondents say they know the non-planned expense of medical device operating system patches. Given the prevalence and importance of medical devices in patient care and risks associated from cyberattacks, these results are very concerning.

Figure 6. Effectiveness in reducing healthcare risks
10-point scale from 1 = ineffective to 10 = very effective below each question, 7+ responses presented



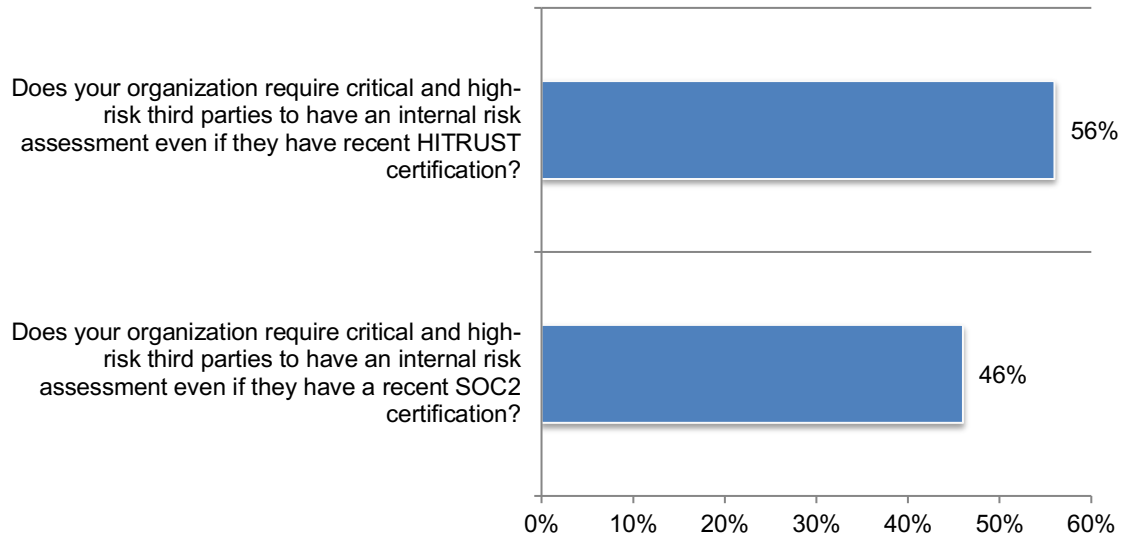
Only 15 percent of respondents say their HDOs conduct annual re-assessments of third-party products and services. According to Figure 7, also concerning is that 53 percent of respondents say these re-assessments are conducted only on-demand or on no regular schedule.

Figure 7. How often do you conduct re-assessments of third parties' products and services?



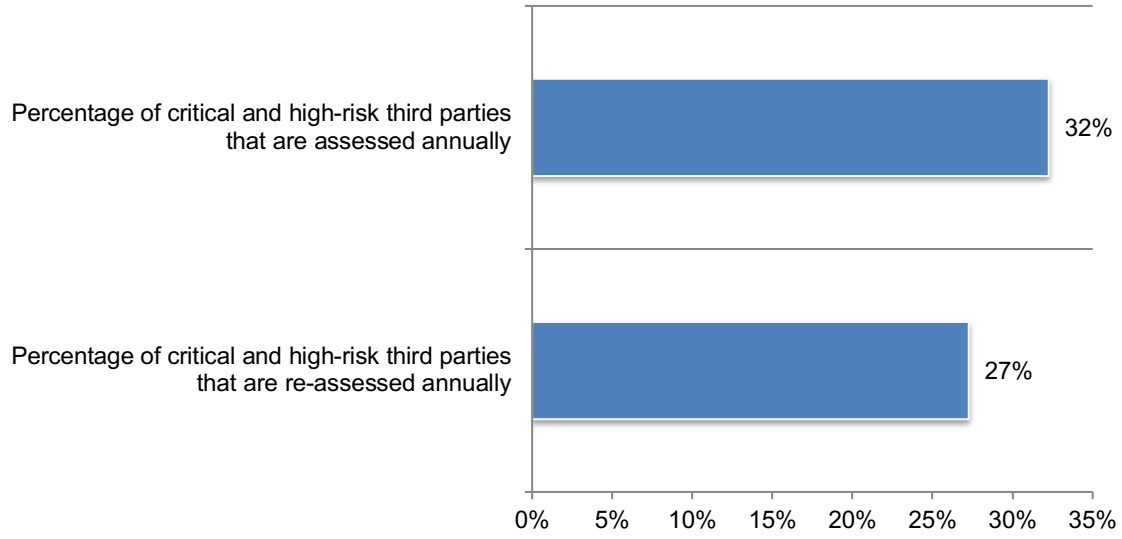
Certifications do not necessarily replace the need for an assessment. As shown in Figure 8, HITRUST and SOC2 certifications do not necessarily eliminate the need for an internal risk assessment. Fifty-six percent of respondents say an internal assessment is required even if they had a recent HITRUST certification. Forty-six percent of respondents say even if they have a recent SOC2 certification, they still need to be assessed.

Figure 8. Does your organization require critical and high-risk third parties to have an internal risk assessment even if they have a recent SOC2 and/or HITRUST certification?
Yes responses presented



Healthcare organizations are at risk because the most critical and high-risk third parties are not assessed or re-assessed annually. Sixty-five percent of respondents say their organizations would assess the risk of all of their vendors and products and services regardless of a pre-assessment label of critical, high, medium, or low. However, as shown in Figure 9, only an average of 32 percent of critical and high-risk third parties are assessed annually, and even fewer are re-assessed annually.

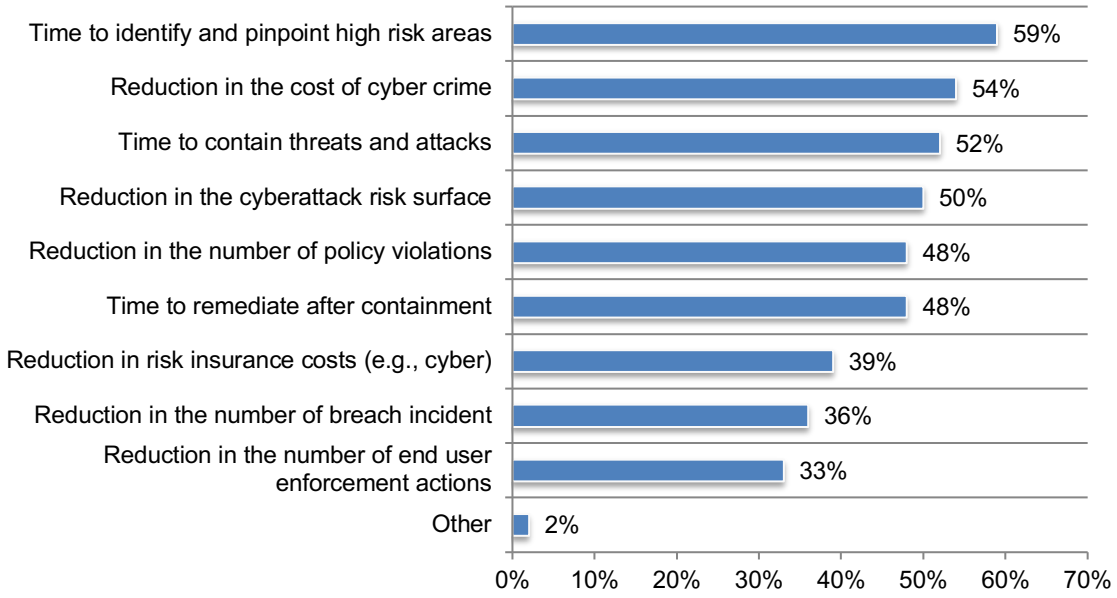
Figure 9. The percentage of critical and high-risk third parties assessed and re-assessed annually
Extrapolated values presented



Third-party vendor risk management programs and relationships

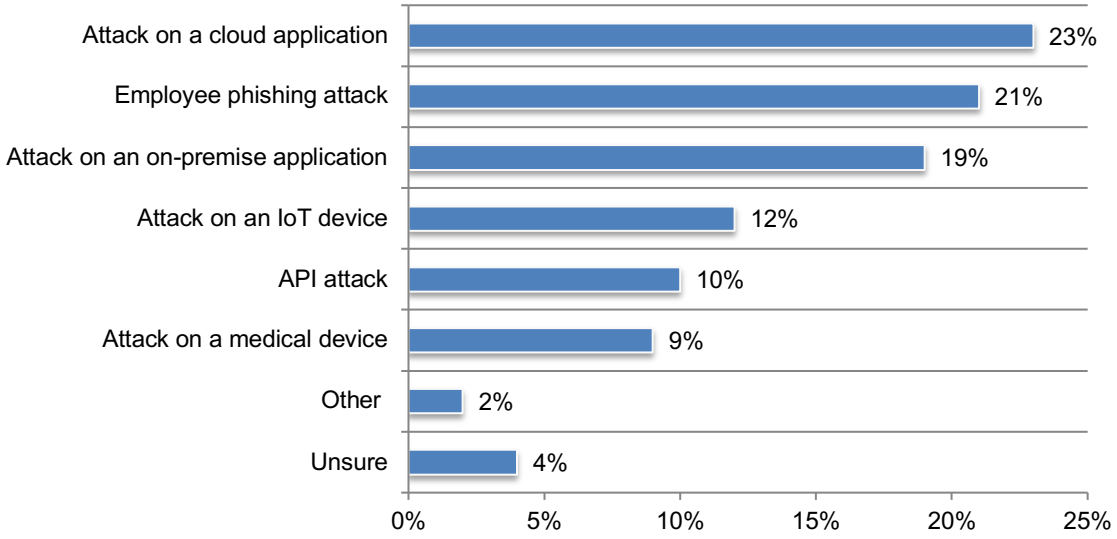
In healthcare, time is of the essence in managing third-party risks. Figure 10 presents a list of metrics used to assess the effectiveness of third-party risk program efforts. As shown, the number one metric is the time to identify and pinpoint high-risk areas (59 percent of respondents), followed by the reduction in the cost of cybercrime (54 percent of respondents) and the time to contain threats and attacks (52 percent of respondents).

Figure 10. Metrics used to assess the effectiveness of third-party vendor risk program efforts
More than one response permitted



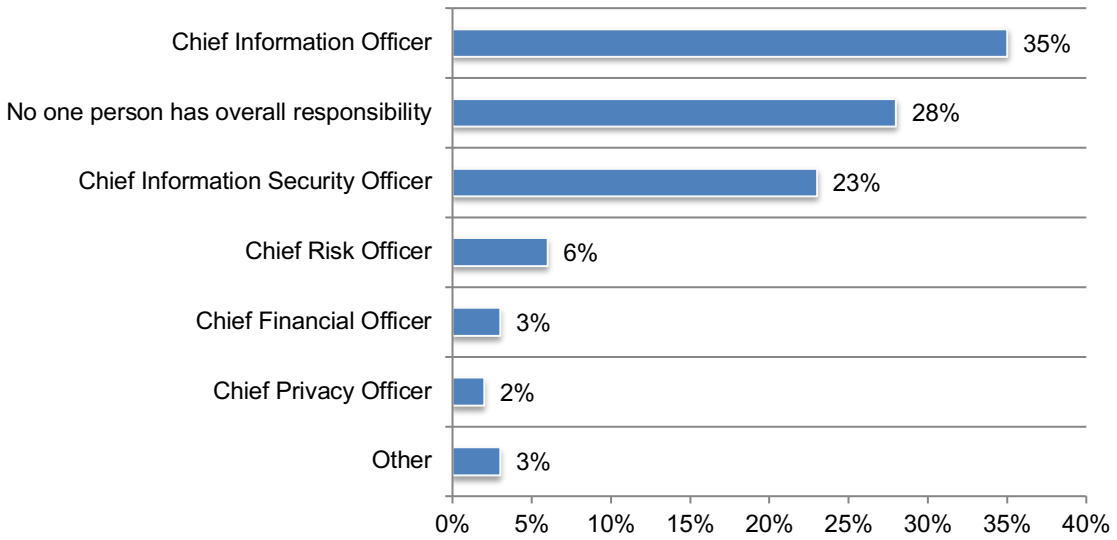
The majority of respondents (60 percent) say their HDOs had a data breach in the past two years involving 28,505 records and costing an average of $837,750. As shown in Figure 11, cloud application and employee phishing attacks were the primary root causes of these breaches.

Figure 11. What was the root cause of the data breach?
Only one choice permitted



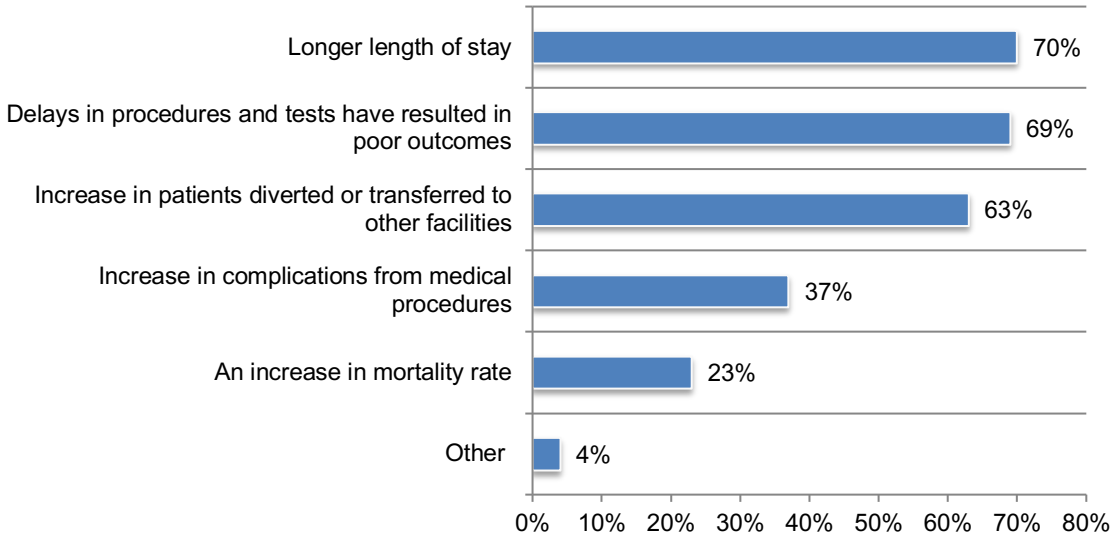
The ability to execute an enterprise-wide risk management strategy is affected by not assigning accountability and ownership to one role. While 35 percent of respondents say the chief information officer has overall responsibility for the third-party risk management program and strategy, 28 percent say no one person has overall responsibility, as shown in Figure 12.

Figure 12. Who has overall responsibility for your organization's risk management approach or strategy?
Only one choice permitted



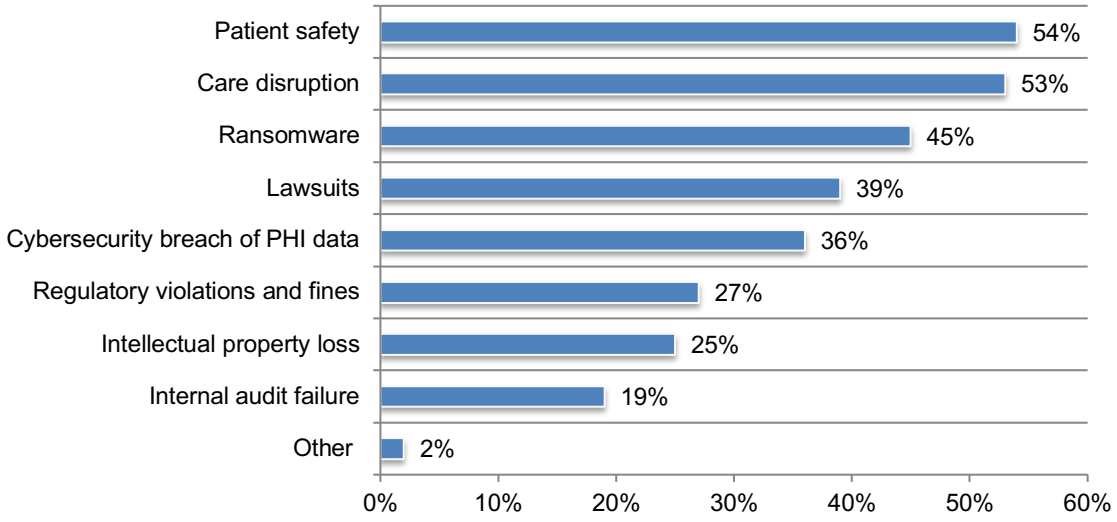
The possible adverse impact on patient care due to third-party risks is the biggest pain point in organizations. As shown in Figure 13, cyberattacks have resulted in more extended hospital stays and delays in procedures and tests that have resulted in poor outcomes. Seventy percent of respondents believe cyberattacks have resulted in a longer length of stay in the hospital, 69 percent of respondents say delays in procedures and tests have resulted in poor outcomes and 63 percent of respondents say it caused an increase in patients having to be diverted or transferred to other facilities. Twenty-three percent of respondents say cyberattacks increased the mortality rate.

Figure 13. The consequences of cyberattacks on patient care
More than one response permitted



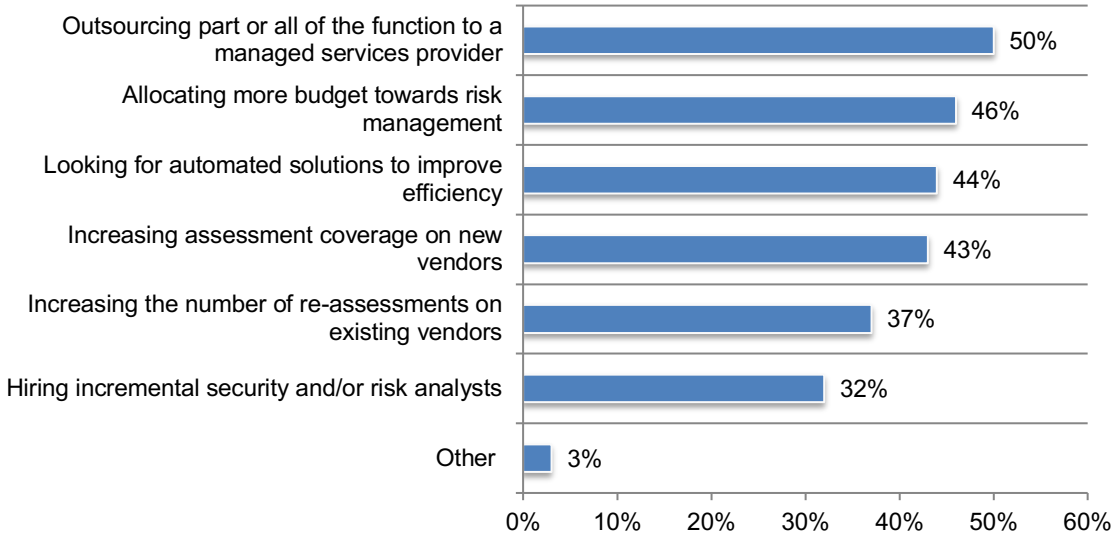
According to Figure 14, patient safety (54 percent of respondents) and care disruption (53 percent of respondents) are a greater concern than such security threats as ransomware (45 percent of respondents) and the breach of PHI data (36 percent of respondents).

Figure 14. What are your biggest concerns or "pain points" resulting from your organization's current third-party risk management program?
Three responses permitted



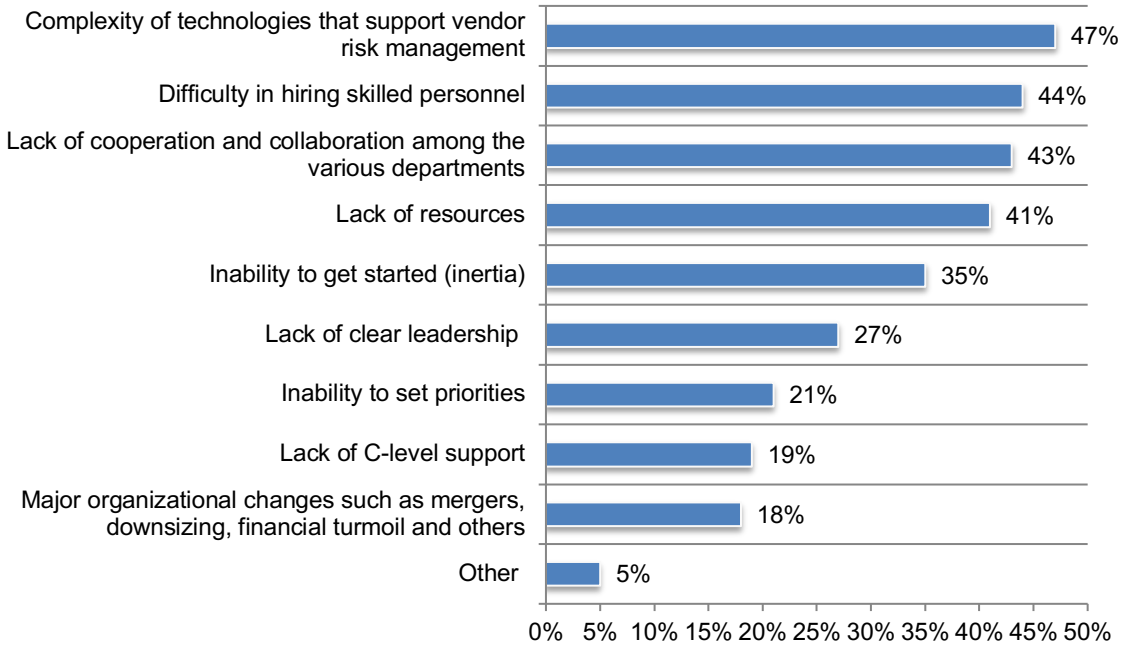
To deal with these pain points, organizations are taking steps to increase support and resources for the third-party risk management program. According to Figure 15, 50 percent of respondents say they are outsourcing part or all of the program to a managed services provider, allocating more budget for risk management (48 percent of respondents) looking for automated solutions to improve efficiency.

Figure 15. What actions is your organization taking to alleviate these pain points?
More than one response permitted



Complexity of technologies and lack of skilled personnel are the most significant barriers to having an effective vendor risk management program. As discussed previously, the number one step taken to alleviate the pain points is to outsource the risk management program to a managed service provider. According to Figure 16, the reasons for outsourcing include the complexity of technologies that support vendor risk management (47 percent of respondents) and difficulty in hiring skilled personnel (44 percent of respondents).

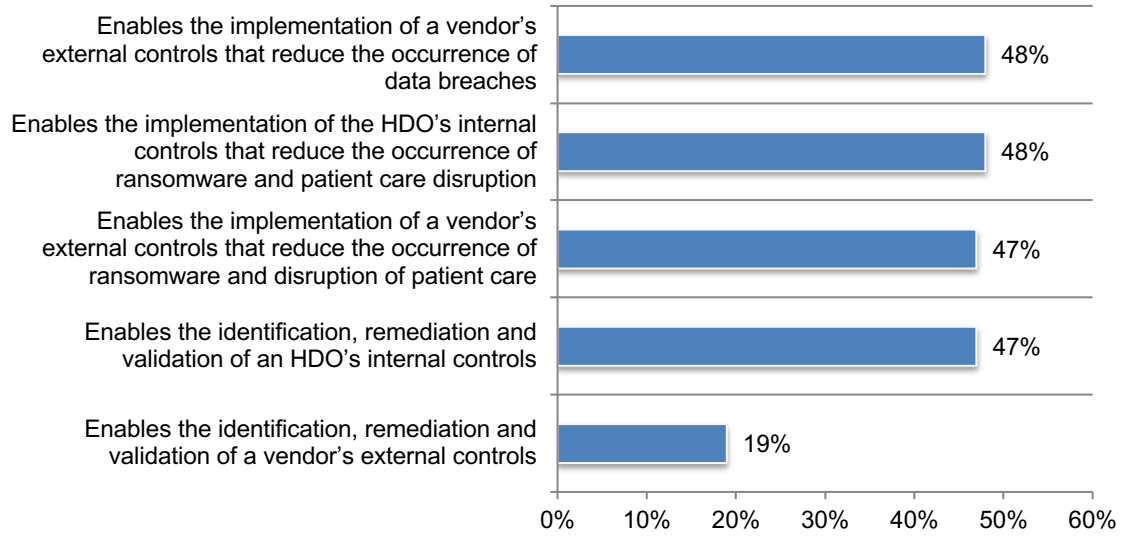
Figure 16. What are the biggest barriers to achieving your organization's vendor risk management objectives?
Three responses permitted



Improvement needs to be made in the controls used to reduce vendor risk. In the context of this research, **internal controls** are an HDO's policies and procedures used to reduce its risks and threats. **External controls** are policies and procedures an HDO's vendor uses to reduce its risk.

Figure 17 presents the characteristics of these controls used by an HDO to reduce vendor risk. Most organizations' internal and external controls are able to reduce vendor risk. Specifically, less than half of respondents (48 percent) believe that their organizations can implement a vendor's external controls that reduce the occurrence of data breaches or implement internal controls that reduce the occurrence of ransomware and patient care disruption. Only 19 percent of respondents say it enables the identification, remediation, and validation of a vendor's external controls.

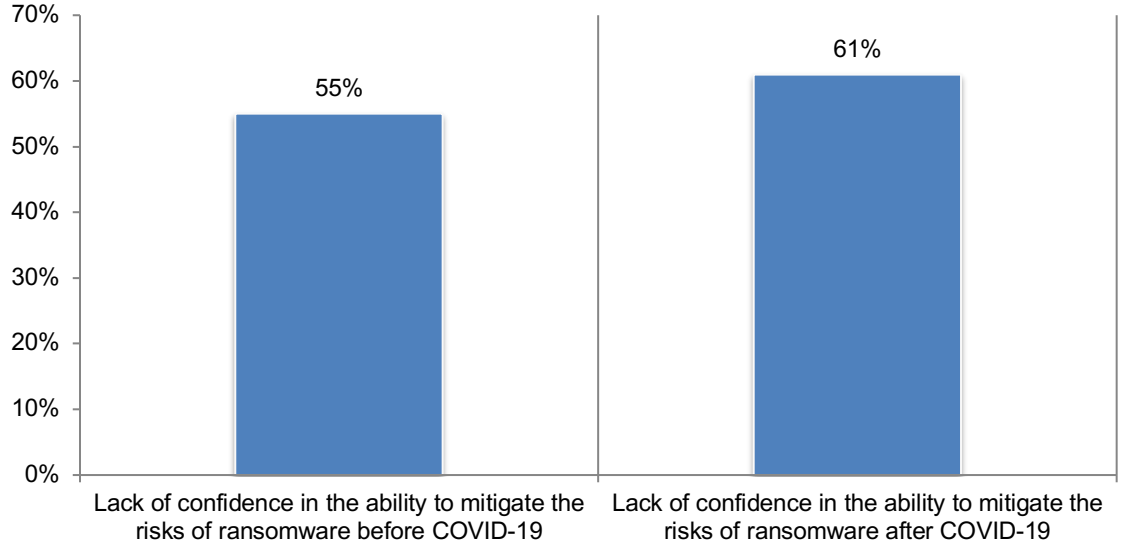
Figure 17. Characteristics of organizations' internal and external controls used by an HDO to reduce vendor risk
Strongly agree and Agree responses presented



Impact of cyberattacks, such as ransomware, patient care

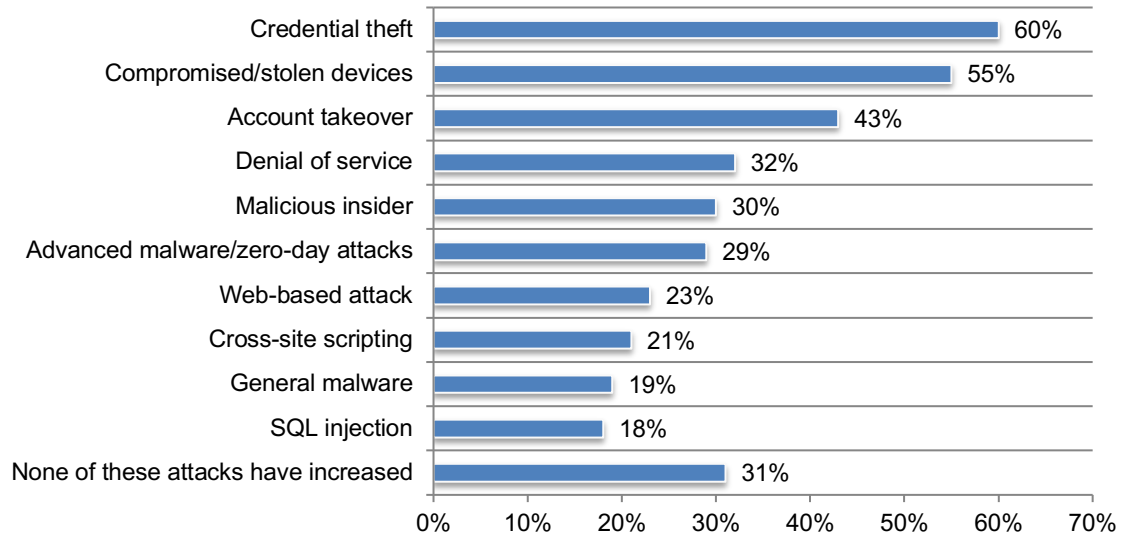
COVID-19 affects organizations' ability to mitigate the risks of patient care. As shown in Figure 18, the lack of confidence in the ability to reduce the risks of ransomware has increased since COVID-19.

Figure 18. How less confident was your organization in its ability to mitigate the risks of ransomware before COVID-19, vs today?
Not confident and no confidence combined



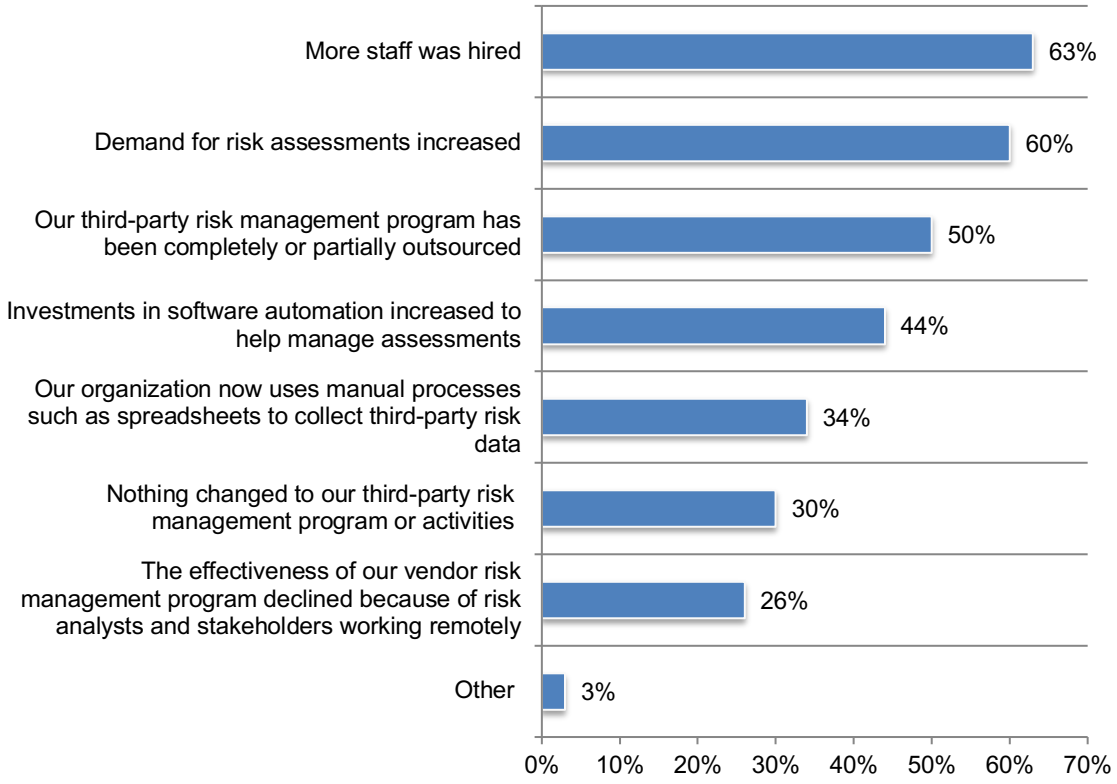
Credential theft and compromised devices have increased since COVID-19. COVID-19 has had a direct impact on the ability to manage third-party risk. According to Figure 19, the cyberattacks that have increased most are credential theft (60 percent of respondents) and compromised/stolen devices (55 percent of respondents).

Figure 19. Since COVID-19, which cyberattacks have increased?
More than one response permitted



An increase in staff and more risk assessments were demanded as a result of COVID-19. Sixty-nine percent of respondents say COVID-19 directly impacted their organizations' ability to manage third-party risk. As shown in Figure 20, more staff was hired (63 percent of respondents), demand for risk assessments increased (60 percent of respondents), and 50 percent of respondents say their third-party risk management program has been completely or partially outsourced. Only 30 percent of respondents say nothing has changed to their third-party risk management program or activities.

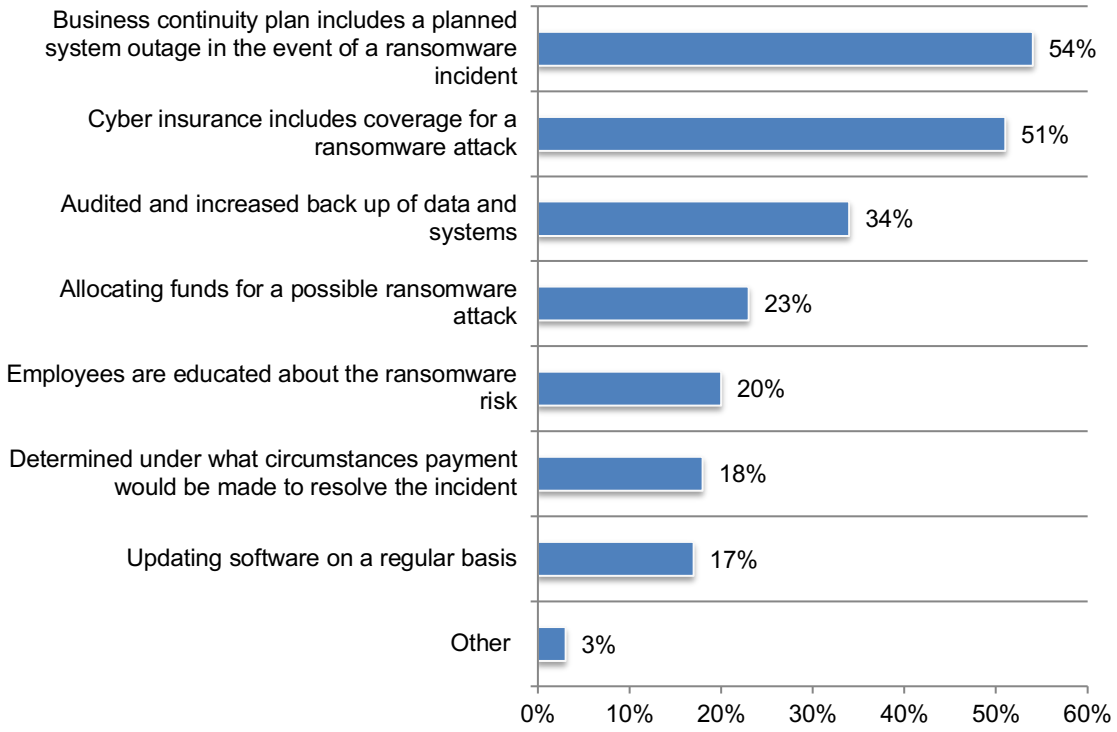
Figure 20. How organizations responded to COVID-19 and the third-party risk
More than one response permitted



Many organizations have experienced an average of two ransomware attacks in the past two years. Forty-three percent of organizations experienced an average of two ransomware attacks in the past two years. Thirty-six percent of respondents say a third party caused these incidents.

As shown in Figure 21, the most important steps taken are having business continuity plans that include a planned system outage in the event of a ransomware attack (54 percent of respondents), and cyber insurance includes coverage for a ransomware attack (51 percent of respondents).

Figure 21. What steps were taken to prepare for a ransomware attack?
More than one response permitted



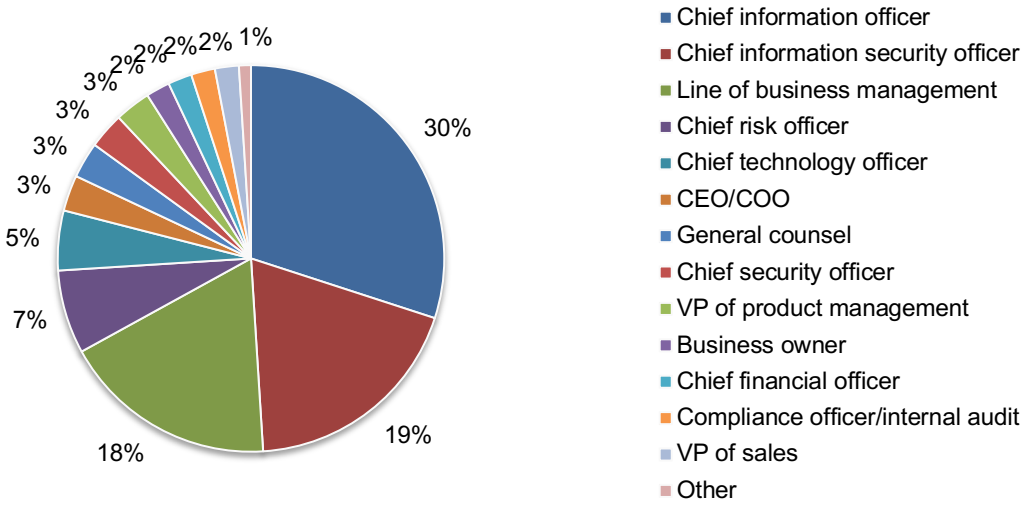
Part 2. Methodology

A sampling frame of 16,540 IT and IT security practitioners in HDO's were selected as participants in this survey. Table 1 shows 664 total returns. Screening and reliability checks required the removal of 67 surveys. Our final sample consisted of 597 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,540	100%
Total returns	664	4.0%
Rejected or screened surveys	67	0.4%
Final sample	597	3.6%

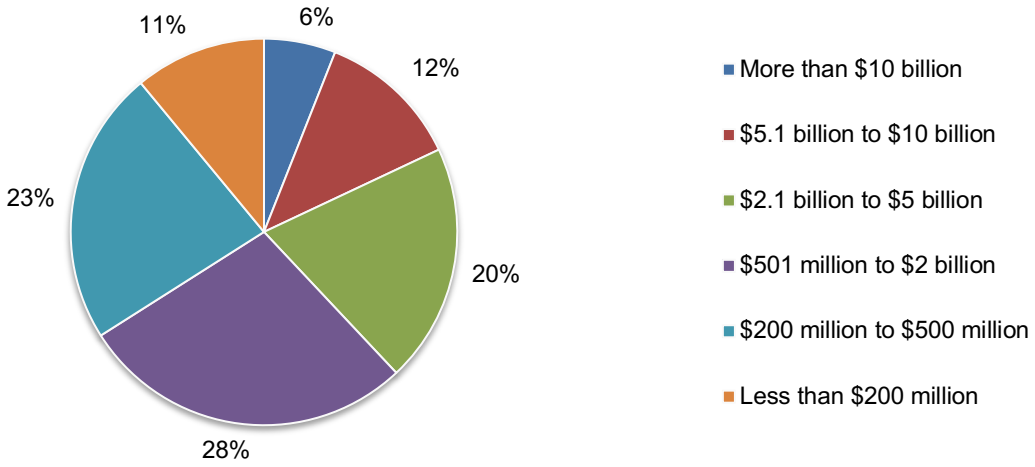
Pie Chart 1 reports the primary person the respondent reports to within the organization. Thirty percent of respondents report to the chief information officer, nineteen percent of respondents report to the chief information security officer, and 18 percent of respondents report to the line of business management, as shown in Pie Chart 1.

Pie Chart 1. Primary person respondent reports to within the organization



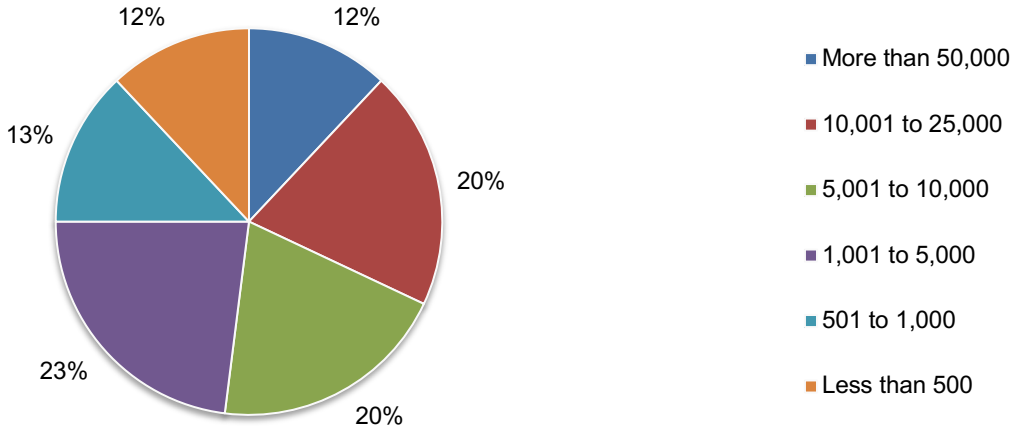
Sixty-six percent of respondents are from organizations with a global revenue of more than $500 million, as shown in Pie Chart 2.

Pie Chart 2. Worldwide revenue of respondent's organization



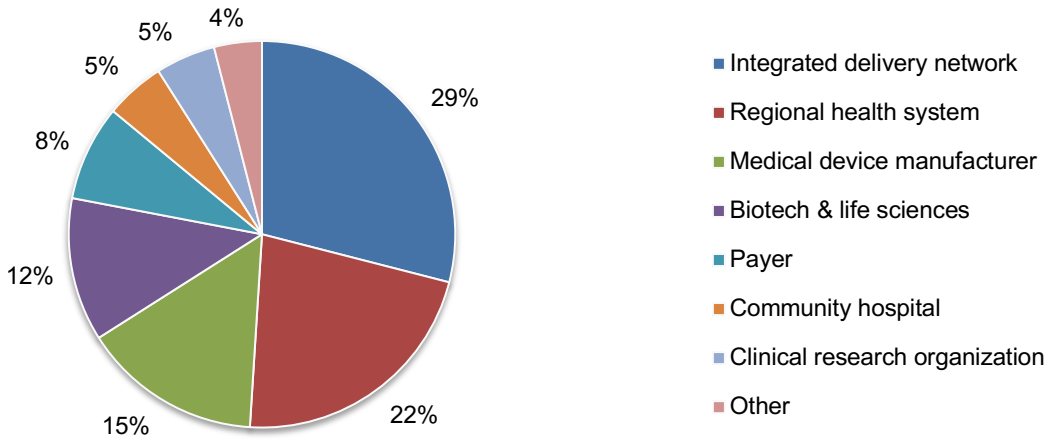
More than half (52 percent) of respondents are from HDO organizations with an employee headcount of more than 5,000 employees, as shown in Pie Chart 3.

Pie Chart 3. The number of employees within the respondent's HDO organization



Pie Chart 4 identifies the type of organizations in which the respondents are located. Twenty-nine percent of respondents are employed in organizations that are integrated delivery networks. This is followed by regional health systems (22 percent of respondents), medical device manufacturers (15 percent of respondents), and biotech and life sciences (12 percent of respondents).

Pie Chart 4. The type of respondent's organization



Part 3. 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 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 and IT security practitioners located in HDO organizations. We also acknowledge that the results may be biased by external events such as media coverage. Finally, 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, 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 May 2021.

Survey response	Freq
Total sampling frame	16,540
Total returned surveys	664
Rejected surveys	67
Final survey	597
Response rate	3.6%

Part 1. Screening questions

S1. Is your healthcare organization an HDO as defined above?	Pct%
Yes	100%
No (Stop)	0%
Total	100%

S2. How familiar are you with your organization's vendor risk management program?	Pct%
Very familiar	44%
Familiar	38%
Somewhat familiar	18%
Not familiar (Stop)	0%
Total	100%

Part 2. Third-party vendor risk management program

Following are seven steps organizations normally take to assess and prioritize vendor risks. Please rate your organization's state of accomplishment for each step using the four-point scale provided below each item.	
Q1a. **Identify key information**. Identify what information is important to the organization and where that information is located.	Pct%
Not attempted	21%
Not accomplished	13%
Partially accomplished	31%
Fully accomplished	35%
Total	100%

Q1b. **Categorize information.** Once identified, the information should be categorized in accordance with its criticality to the organization.	Pct%
Not attempted	18%
Not accomplished	15%
Partially accomplished	35%
Fully accomplished	32%
Total	100%

Q1c. **Identify threats.** Look at the various threats (and sources of threats) that are posed against the organization and its assets and vulnerabilities.	Pct%
Not attempted	20%
Not accomplished	17%
Partially accomplished	37%
Fully accomplished	26%
Total	100%

Q1d. **Assess and prioritize vulnerabilities**. Identify and prioritize vulnerabilities in existing controls and ascertain the likelihood that they will be exploited and the potential impact of an incident.	Pct%
Not attempted	16%
Not accomplished	19%
Partially accomplished	40%
Fully accomplished	25%
Total	100%

Q1e. **Assess the risks.** Risks posed against the organization can be determined by examining the various threats, the source of threats, the likelihood a threat will materialize and the impact a threat will have on the protected information.	Pct%
Not attempted	12%
Not accomplished	10%
Partially accomplished	43%
Fully accomplished	35%
Total	100%

Q1f. **Identify controls.** Identify what specific controls are needed at the various layers to ensure all risks are at a level acceptable to the business.	Pct%
Not attempted	9%
Not accomplished	13%
Partially accomplished	34%
Fully accomplished	44%
Total	100%

Q1g. **Monitor continuously.** It is important that the risk-based approach is a continuous process that evolves with business goals.	Pct%
Not attempted	23%
Not accomplished	27%
Partially accomplished	25%
Fully accomplished	25%
Total	100%

Q2a. What are your biggest concerns or "pain points" resulting from your organization's current third-party risk management program? Please select your top three choices.	Pct%
Care disruption	53%
Cybersecurity breach of PHI data	36%
Intellectual property loss	25%
Internal audit failure	19%
Lawsuits	39%
Patient safety	54%
Ransomware	45%
Regulatory violations and fines	27%
Other (please specify)	2%
Total	300%

Q2b. What actions is your organization taking to alleviate the concerns listed above? Please select all that apply.	Pct%
Allocating more budget towards risk management	46%
Increasing assessment coverage on new vendors	43%
Hiring incremental security and/or risk analysts	32%
Increasing the number of re-assessments on existing vendors	37%
Looking for automated solutions to improve efficiency	44%
Outsourcing part or all of the function to a managed services provider	50%
Other (please specify)	3%
Total	255%

Q3. What are the biggest barriers to achieving your organization's vendor risk management objectives? Please select the top three barriers only.	Pct%
Complexity of technologies that support vendor risk management	47%
Difficulty in hiring skilled personnel	44%
Inability to get started (inertia)	35%
Inability to set priorities	21%
Lack of C-level support	19%
Lack of clear leadership	27%
Lack of cooperation and collaboration among the various departments	43%
Lack of resources	41%
Major organizational changes such as mergers, downsizing, financial turmoil and others	18%
Other (please specify)	5%
Total	300%

For the following questions, please use the 10-point scale from 1 = ineffective to 10 = very effective below each question.	
Q4a. How effective and accurate are the risk assessment questionnaires in determining your risk profile?	Pct%
1 or 2	23%
3 or 4	24%
5 or 6	21%
7 or 8	20%
9 or 10	12%
Total	100%
Extrapolated value	4.98

Q4b. How effective is your organization in knowing where all of its medical devices are?	Pct%
1 or 2	20%
3 or 4	27%
5 or 6	17%
7 or 8	21%
9 or 10	15%
Total	100%
Extrapolated value	5.18

Q4c. How effective is your organization in knowing when a medical device vendor's operating device is end of life or out-of-date?	Pct%
1 or 2	16%
3 or 4	28%
5 or 6	21%
7 or 8	23%
9 or 10	12%
Total	100%
Extrapolated value	5.24

Q4d. How effective is your organization in knowing the non-planned expense of medical device operating system patches?	Pct%
1 or 2	23%
3 or 4	20%
5 or 6	28%
7 or 8	13%
9 or 10	16%
Total	100%
Extrapolated value	5.08

Q4e. How effective is your organization in knowing how many of its PHI records are accessed, transmitted or stored by third-party products or services?	Pct%
1 or 2	19%
3 or 4	17%
5 or 6	25%
7 or 8	23%
9 or 10	16%
Total	100%
Extrapolated value	5.50

Q5. What metrics are used by your organization to assess the effectiveness of its third-party risk program efforts? Please select all that apply.	Pct%
Time to identify and pinpoint high risk areas	59%
Time to contain threats and attacks	52%
Time to remediate after containment	48%
Reduction in risk insurance costs (e.g., cyber)	39%
Reduction in the cyberattack risk surface	50%
Reduction in unplanned system downtime	60%
Reduction in the number of policy violations	48%
Reduction in the number of end user enforcement actions	33%
Reduction in the number of breach incident	36%
Reduction in the cost of cyber crime	54%
Other (please specify)	2%
Total	481%

Q6. How often do you conduct re-assessments of your third-parties' products and services?	Pct%
Real-time	12%
Monthly	12%
Quarterly	8%
Annually	15%
On-demand	23%
No regular schedule	30%
Total	100%

Q7. Did your organization take any of the following actions when gaps in a third-party's privacy and security practices and policies were discovered? Please select all that apply.	Pct%
Assisted the third party in improving their privacy and security practices	50%
Required a third party to remediate the gap	51%
Required the third party to conduct an external audit	39%
Required the third party to purchase cyber risk insurance	47%
Selected another third party due to risk	44%
No actions were taken	25%
Other (please specify)	3%
Total	259%

Q8. Does your organization require critical and high-risk third parties to have an **internal** risk assessment even if they have a recent SOC2 certification?	Pct%
Yes	46%
No	54%
Total	100%

Q9. Does your organization require critical and high-risk third parties to have an **internal** risk assessment even if they have recent HITRUST certification?	Pct%
Yes	56%
No	44%
Total	100%

Part 3. Third-party risk management program assessment

Q10. If you had the resources and money, would your organization assess the risks of ALL of its vendors and products/services, regardless of a pre-assessment label of critical, high, medium or low?	Pct%
Yes	65%
No	35%
Total	100%

Q11. What is the percentage of your organization's critical and high-risk third parties are **assessed** annually?	Pct%
Zero	11%
1% to 25%	38%
26% to 50%	27%
51% to 75%	15%
76% to 100%	9%
Total	100%
Extrapolated value	32%

Q12. What is the percentage of your organization's critical and high-risk third parties are **re-assessed** annually?	Pct%
Zero	15%
1% to 25%	41%
26% to 50%	27%
51% to 75%	12%
76% to 100%	5%
Total	100%
Extrapolated value	27%

Part 4. Attributions

Please rate the following statements regarding the capabilities of your organization's vendor risk program using the agreement scale provided below each item. In the context of this research, **internal controls** are an HDO's policies and procedures used to reduce its risks and threats. **External controls** are policies and procedures an HDO's vendor uses to reduce their risk.	
Q13a. It runs on spreadsheets, email and phone calls	Pct%
Strongly agree	30%
Agree	23%
Unsure	15%
Disagree	18%
Strongly disagree	14%
Total	100%

Q13b. It enables the implementation of the HDO's **internal** controls that reduce the occurrence of ransomware and patient care disruption.	Pct%
Strongly agree	23%
Agree	25%
Unsure	15%
Disagree	21%
Strongly disagree	16%
Total	100%

Q13c. It enables the identification, remediation and validation of an HDO's **internal** controls.	Pct%
Strongly agree	26%
Agree	21%
Unsure	16%
Disagree	20%
Strongly disagree	17%
Total	100%

Q13d. It enables the implementation of a vendor's **external** controls that reduce the occurrence of data breaches.	Pct%
Strongly agree	23%
Agree	25%
Unsure	14%
Disagree	23%
Strongly disagree	15%
Total	100%

Q13e. It enables the implementation of a vendor's **external** controls that reduce the occurrence of ransomware and disruption of patient care.	Pct%
Strongly agree	21%
Agree	26%
Unsure	16%
Disagree	24%
Strongly disagree	13%
Total	100%

Q13f. It enables the identification, remediation and validation of a vendor's **external** controls.	Pct%
Strongly agree	19%
Agree	30%
Unsure	14%
Disagree	26%
Strongly disagree	11%
Total	100%

Q13g. It enables the assessment of fourth-parties' vendor products and services. A fourth party provides products and services to an HDO's direct, third-party vendor.	Pct%
Strongly agree	25%
Agree	29%
Unsure	19%
Disagree	15%
Strongly disagree	12%
Total	100%

Q13h. Our organization's leaders always accept our recommendations and never allow contracts with a third party that presents a high risk to the health system.	Pct%
Strongly agree	20%
Agree	18%
Unsure	15%
Disagree	31%
Strongly disagree	16%
Total	100%

Q13i. Our organization always completes a risk assessment of its third parties prior to contracting with them.	Pct%
Strongly agree	19%
Agree	21%
Unsure	12%
Disagree	33%
Strongly disagree	15%
Total	100%

Part 5. Background on vendor relationships

Q14. Today, approximately, how many third parties does your organization contract with for products and services?	Pct%
Less than 250	13%
250 to 500	23%
501 to 1,000	11%
1,001 to 2,500	26%
2,501 to 5,000	20%
5,001 to 10,000	5%
More than 10,000	2%
Total	100%
Extrapolated value	1,950

Q15. What percentage of these third parties have access to your organization's PHI?	Pct%
Less than 5 percent	4%
6 percent to 10 percent	13%
11 percent to 25 percent	16%
26 percent to 50 percent	25%
51 percent to 75 percent	27%
76 percent to 100 percent	15%
Total	100%
Extrapolated value	43%

Q16. Approximately how many of these third parties has your organization assessed?	Pct%
Less than 250	25%
250 to 500	13%
501 to 1,000	26%
1,001 to 2,500	25%
2,501 to 5,000	7%
5,001 to 10,000	3%
More than 10,000	1%
Total	100%
Extrapolated value	1,276.25

Q17. In the next 12 months, how many third parties will your organization contract with for their products and services?	Pct%
Less than 250	16%
250 to 500	17%
501 to 1,000	23%
1,001 to 2,500	12%
2,501 to 5,000	13%
5,001 to 10,000	15%
More than 10,000	4%
Total	100%
Extrapolated value	2,541

Q18. What percentage of these third parties will have access to your organization's PHI over the next 12 months?	Pct%
Less than 5 percent	27%
6 percent to 10 percent	29%
11 percent to 25 percent	18%
26 percent to 50 percent	15%
51 percent to 75 percent	7%
76 percent to 100 percent	4%
Total	100%
Extrapolated value	20%

Q19. Approximately how many of these third parties will your organization assess over the next 12 months?	Pct%
Less than 250	34%
250 to 500	29%
501 to 1,000	16%
1,001 to 2,500	13%
2,501 to 5,000	8%
5,001 to 10,000	0%
More than 10,000	0%
Total	100%
Extrapolated value	791.75

Part 6. The impact to vendor risk programs due to COVID-19

Q20. Did COVID-19 have a direct impact on your organization's ability to manage third-party risk?	Pct%
Yes	69%
No (please skip to Q22)	31%
Total	100%

Q21. If yes, what changes did your organization experience following COVID-19? Please select all that apply.	Pct%
Our organization now uses manual processes such as spreadsheets to collect third-party risk data	34%
The effectiveness of our vendor risk management program declined because of risk analysts and stakeholders working remotely	26%
Investments in software automation increased to help manage assessments	44%
Our third-party risk management program has been completely or partially outsourced	50%
Demand for risk assessments increased	60%
More staff was hired	63%
Nothing changed to our third-party risk management program or activities	30%
Other (please specify)	3%
Total	310%

Q22. Since COVID-19, have any of the following attacks i**ncreased**? Please select all that apply.	Pct%
Account takeover	43%
Advanced malware/zero-day attacks	29%
Compromised/stolen devices	55%
Credential theft	60%
Cross-site scripting	21%
Denial of service	32%
General malware	19%
Malicious insider	30%
SQL injection	18%
Web-based attack	23%
None of these attacks have increased	31%
Total	361%

Q23a. Do you believe cyberattacks on your organization have had an adverse impact on patient care?	Pct%
Yes	56%
No (please skip to Q24a)	44%
Total	100%

Q23b. If yes, has your organization experienced any of the following? Please select all that apply.	Pct%
An increase in mortality rate	23%
Delays in procedures and tests have resulted in poor outcomes	69%
Increase in complications from medical procedures	37%
Increase in patients diverted or transferred to other facilities	63%
Longer length of stay	70%
Other (please specify)	4%
Total	266%

Part 7. Third-party data breaches

Q24a. Has your organization experienced one or more data breaches caused by one of its third parties?	Pct%
Yes	60%
No (please skip to Q28)	34%
Unsure (please skip Q28)	6%
Total	100%

Q24b. If yes, how many of these incidents did your experience have over the past 2 years?	Pct%
One	43%
2 to 5	37%
6 to 10	17%
More than 10	3%
Total	100%
Extrapolated value	3.4

Q25. How many records were lost or stolen as a result of these data breaches?	Pct%
Less than 100	28%
100 to 1,000	31%
1,001 to 5,000	24%
5,001 to 10,000	12%
10,001 to 50,000	9%
50,001 to 100,000	8%
100,001 to 250,000	6%
250,001 to 500,000	2%
More than 500,000	0%
Total	120%
Extrapolated value	28,505

Q26. What was the root cause of the data breach?	Pct%
API attack	10%
Attack on a cloud application	23%
Attack on a medical device	9%
Attack on an IoT device	12%
Attack on an on-premise application	19%
Employee phishing attack	21%
Other (please specify)	2%
Unsure	4%
Total	100%

Q27. Please provide your best estimate for the total cost of these data breaches over the past 2 years.	Pct%
Less than $50,000	28%
$50,000 to $100,000	27%
$100,001 to $500,000	21%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	8%
$5,000,001 to $10,000,000	2%
$10,000,001 to $25,000,000	0%
More than $25,000,000	1%
Total	100%
Extrapolated value	$ 837,750

Part 8. Impact of ransomware

Q28. Have you taken the following steps to prepare for a ransomware attack? Please select all that apply.	Pct%
Allocating funds for a possible ransomware attack	23%
Audited and increased back up of data and systems	34%
Business continuity plan includes a planned system outage in the event of a ransomware incident	54%
Cyber insurance includes coverage for a ransomware attack	51%
Determined under what circumstances payment would be made to resolve the incident	18%
Employees are educated about the ransomware risk	20%
Updating software on a regular basis	17%
Other (please specify)	3%
Total	220%

Q29. Did your organization **ever** experience a ransomware attack?	Pct%
Yes	43%
No (please skip to Q36)	51%
Unsure (please skip to Q36)	6%
Total	100%

Q30. How many ransomware incidents did your organization experience over the past two years?	Pct%
One	67%
Two to five	31%
Six to 10	2%
More than 10	0%
Total	100%
Extrapolated value	1.9

Q31. Were any of these incidents caused by a third party?	Pct%
Yes	36%
No	55%
Unsure	9%
Total	100%

Q32a. Did your organization pay the ransom?	Pct%
Yes	60%
No	40%
Total	100%

Q32b. If yes, how much was the ransom? If your organization has had more than one ransomware attack, please select the costliest ransom.	Pct%
Less than $10,000	25%
$10,000 to $25,000	21%
$25,001 to $50,000	12%
$50,001 to $75,000	9%
$75,001 to $100,000	11%
$100,001 to $250,000	6%
$250,001 to $500,000	8%
$500,001 to $1,000,000	5%
$1,00,001 to $5,000,000	1%
$5,00,001 to $10,000,000	2%
More than $10,000,000	0%
Total	100%
Extrapolated value	$ 282,675

Q33. What was the duration of the ransomware disruption?	Pct%
Less than 1 day	40%
1 day to 7 days	46%
8 days to 14 days	7%
15 days to 30 days	5%
More than 30 days	2%
Total	100%
Extrapolated value (days)	4.66

Q34a. Did the ransomware attack result in a disruption in patient care operations?	Pct%
Yes	45%
No	50%
Unsure	5%
Total	100%

Q34b. If yes, what impact did the ransomware attack have on patient care? Please select all that apply.	Pct%
An increase in mortality rate	22%
Delays in procedures and tests have resulted in poor outcomes	70%
Increase in complications from medical procedures	36%
Increase in patients transferred or diverted to other facilities	65%
Longer length of stay	71%
Other (please specify)	4%
Total	268%

Q35. How confident was your organization in its ability to mitigate the risks of ransomware before COVID-19?	Pct%
Very confident	12%
Confident	14%
Somewhat confident	19%
Not confident	29%
No confidence	26%
Total	100%

Q36. How confident is your organization in its ability to mitigate the risks of ransomware after COVID-19?	Pct%
Very confident	14%
Confident	15%
Somewhat confident	10%
Not confident	37%
No confidence	24%
Total	100%

Part 9. Risk ownership and budget

Q37. Who has overall responsibility for your organization's risk management approach or strategy? Please select only one choice.	Pct%
Chief Risk Officer	6%
Chief Information Officer	35%
Chief Financial Officer	3%
Chief Information Security Officer	23%
Chief Privacy Officer	2%
No one person has overall responsibility	28%
Other (please specify)	3%
Total	100%

Q38a. Does your organization have a formal budget for vendor risk management activities/program?	Pct%
Yes	50%
No (please skip to Part 10)	45%
Unsure (please skip to Part 10)	5%
Total	100%

Q38b. If yes, how much will your organization allocate to investment in vendor risk management automation products and services in the upcoming fiscal year?	Pct%
Less than $250,000	29%
Between $250,000 and $500,000	21%
Between $500,000 and $1 million	22%
Between $1 and $2 million	21%
Between $2 and $5 million	5%
More than $5 million	2%
Total	100%
Extrapolated value	$ 890,000

Part 10: Organizational characteristics

D1. Check the **Primary Person** you report to within the organization	Pct%
CEO/COO	3%
Business owner	2%
Chief financial officer (CFO)	2%
General counsel	3%
Chief information officer (CIO)	30%
Chief technology officer (CTO)	5%
Chief risk officer (CRO)	7%
Chief information security officer (CISO)	19%
Compliance officer/internal audit	2%
Human resources VP	0%
Chief security officer (CSO)	3%
Line of business (LOB) management	18%
VP of sales	2%
VP of product management	3%
Other (please specify)	1%
Total	100%

D2. What range best defines the worldwide revenue of your organization?	Pct%
Less than $200 millions	11%
$200 million to $500 million	23%
$501 million to $2 billion	28%
$2.1 billion to $5 billion	20%
$5.1 billion to $10 billion	12%
More than $10 billion	6%
Total	100%

D3. How many employees are in your HDO organization?	Pct%
Less than 500	12%
501 to 1,000	13%
1,001 to 5,000	23%
5,001 to 10,000	20%
10,001 to 25,000	20%
More than 50,000	12%
Total	100%

D4. What is the type of the organization?	Pct%
Integrated delivery network (IDN)	29%
Regional health system	22%
Community hospital	5%
Clinical research organization (CRO)	5%
Medical device manufacturer	15%
Biotech & life sciences	12%
Payer	8%
Other (please specify)	4%
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.

About the Sponsor

Censinet, based in Boston, MA, enables healthcare organizations to take the risk out of their business with Censinet RiskOps™, the first and only cloud-based exchange that integrates and consolidates enterprise risk management and operations capabilities across critical clinical and business areas.

RiskOps builds upon the Company's foundational success with third-party risk management (TPRM) for healthcare. Censinet transforms healthcare risk by increasing productivity and operational effectiveness while eliminating risks to care delivery, data privacy, and patient safety.

Find out more about Censinet and its RiskOps platform at censinet.com or email us at info@censinet.com.