Ponemon INSTITUTE

The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking

Sponsored by Censinet

Independently conducted by Ponemon Institute LLC

Publication Date: January 2023

The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking

Prepared by Ponemon Institute, January 2023

Part 1. Executive Summary

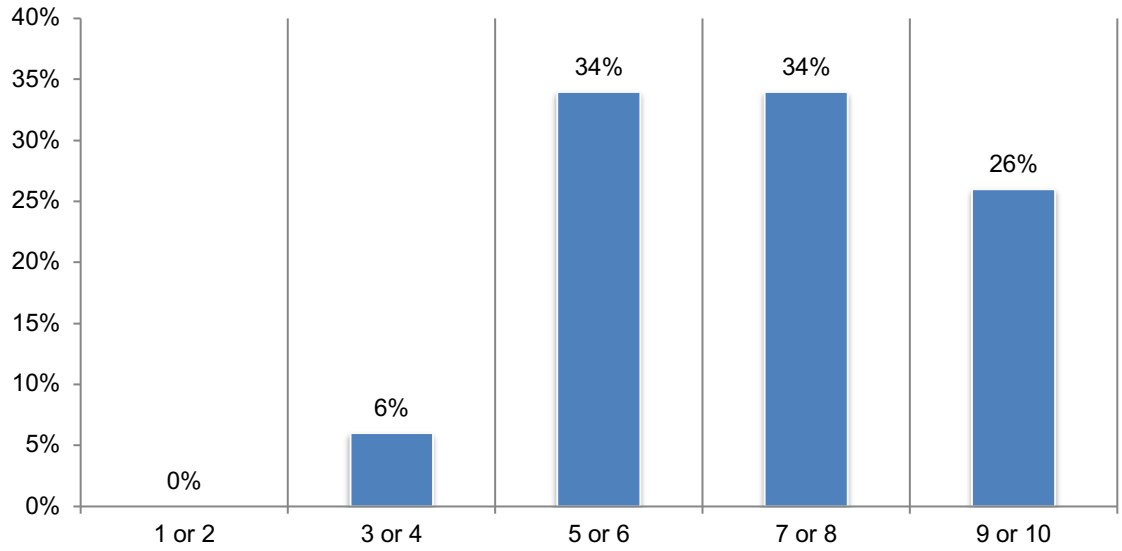
The purpose of this research is to provide an update to the industry's first study on the impact of ransomware on patient safety, titled *The Impact of Ransomware on Healthcare During COVID-19 and Beyond*, September 2021. That seminal study qualitatively demonstrated a correlation between ransomware and various impacts to patient care, including increased patient transfers/diversions, delays in procedures and tests, increased complications from medical procedures, and higher mortality rates. This updated study, according to survey respondents, shows ransomware continues to impact patient care, and seeks to understand how cybersecurity peer benchmarking can help healthcare organizations strengthen their cybersecurity posture to help reduce the risk of a ransomware attack and its potential impact on patient care.

As shown in the 2021 study sponsored by Censinet, 61 percent of respondents were not confident, or had no confidence, in their ability to mitigate the risks of ransomware. In this year's study, also sponsored by Censinet, more organizations experienced a ransomware attack and an increasing number of these attacks are caused by poor cybersecurity controls internally and at third-party vendors and products. In addition to the impact of ransomware on patient safety, this study explores the importance of cybersecurity peer benchmarking and third party risk management to reduce cyber threats such as ransomware.

For example, a key takeaway is that cybersecurity peer benchmarking provides valuable insights into how healthcare resources should be allocated to reduce the risk of ransomware and its potential impacts on patient care. Respondents were asked to rate the value of using benchmarks to understand what amount of funds and resources should be allocated to their cybersecurity programs on a scale of 1 = not valuable to 10 = very valuable. As shown, 60 percent of respondents say they are valuable or very valuable. Benchmarking is also important to making the business case for hiring cyber staff and investing in technologies.

Figure 1. How valuable are peer benchmarks to getting the right level of investment and resources for your organization's cybersecurity program?

On a scale from 1 = not valuable to 10 = very valuable



The two-year trend in ransomware attacks

This research is unique because it tracks how healthcare organizations and patient care have been impacted by ransomware attacks since 2021. The following findings demonstrate that ransomware continues to be a growing problem for the industry.

- **Ransomware attacks are on the rise**. Almost half of respondents (47 percent) say their organizations experienced a ransomware attack in the past two years, an increase from 43 percent in 2021. In the past two years, 93 percent of these respondents experienced at least one (65 percent) or between two and five ransomware attacks (28 percent).

- **Third-party ransomware attacks have increased significantly**. Of the 47 percent of respondents who reported a ransomware attack, 46 percent say it was caused by a third party, an increase from 36 percent in 2021. This finding indicates the importance of having policies and practices in place to proactively assess third party risk, remediate identified security gaps, and quickly respond to and recover from a third party-driven ransomware attack.

- **More organizations are paying ransomware.** Sixty-seven percent of respondents, an increase from 60 percent, say their organizations are paying ransom. The average ransom payment has increased from $282,675 to $352,541 in the past two years. The average duration of disruptions caused by ransomware attacks has not improved and can last more than one month (35 days).

- **More patients are adversely affected by ransomware attacks.** Fifty-three percent of respondents in organizations that had a ransomware attack say it resulted in a disruption in patient care. Complications from medical procedures due to ransomware attacks increased significantly from 36 percent of respondents to 45 percent of respondents.

  The most prevalent impact was an increase in patients transferred or diverted to other facilities from 65 percent of respondents last year to 70 percent of respondents this year. In addition, 21 percent of respondents say ransomware has an adverse impact on patient mortality rates.

- **Business continuity plans are increasingly the most important step to preparing for a ransomware attack.** Sixty percent of respondents say their organizations have a business continuity plan that includes a planned system outage in the event of a ransomware attack, an increase from 54 percent of respondents. Also, 33 percent of respondents say their organization is increasing funds to deal with a potential ransomware attack, an increase from 23 percent in the previous study.

Benchmarking the effectiveness of cybersecurity programs is considered important and valuable.

As ransomware attacks increase, an effective cybersecurity program is critical. According to the findings, respondents agree that peer benchmarking is both valuable and important.

- **Benchmarking is very valuable in demonstrating cybersecurity program effectiveness, according to 78 percent of respondents.** Benchmarking is also valuable when demonstrating cybersecurity framework coverage/compliance (61 percent of respondents) and improving cybersecurity programs (52 percent of respondents).

- **Benchmarking improves cybersecurity program decision making.** Another important value of benchmarking is to make better, data-driven decisions (53 percent of respondents) followed by the ability to demonstrate effectiveness of benchmarking program investments (48 percent of respondents).

- **Benchmarking is important to making the business case for hiring cyber staff and purchasing technologies, according to 69 percent and 60 percent of respondents respectively.** Fifty-seven percent of respondents say benchmarking is valuable when making investment decisions in the cybersecurity program.

- **Benchmarking is important when establishing cybersecurity program goals, according to 67 percent of respondents.** These metrics are also helpful in responding to and recovering from ransomware attacks, according to 51 percent of respondents.

Part 2. 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:

- The value of benchmarking cybersecurity programs to reduce the impact of ransomware
- The two-year trend in the rise of ransomware in healthcare and its impact on patient care
- Third-party risk management program assessment

For this study, Ponemon Institute surveyed 579 IT and IT security professionals in healthcare delivery organizations (HDOs). HDO survey respondents are from entities that deliver clinical care and are familiar with their organization's cybersecurity and risk management programs. These HDOs include integrated delivery networks, regional health systems, community hospitals, physician groups, and payers.

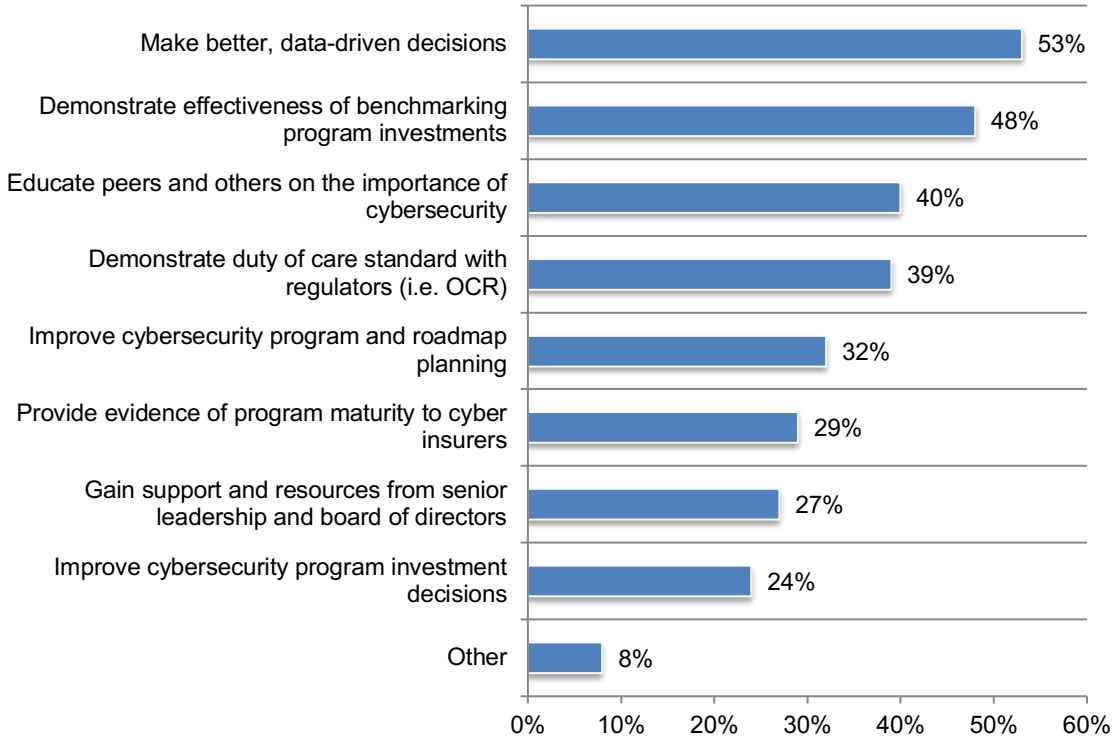
In the context of this research, third parties and vendors are used interchangeably. Third party or vendor risk management is the application of rigorous and systematic analytic techniques to the evaluation of organizational, product, and/or services risks that impact the HDO enterprise, including information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

Cybersecurity benchmarking is defined as the comparison of an HDO's cybersecurity performance and maturity against peer HDO organizations across (1) key cybersecurity program cost, productivity, and operational metrics, and (2) program coverage for industry recognized security practices such as NIST Cybersecurity Framework (NIST CSF) and HHS Health Industry Cybersecurity Practices (HICP).

2.1 The value of benchmarking cybersecurity programs to reduce the impact of ransomware

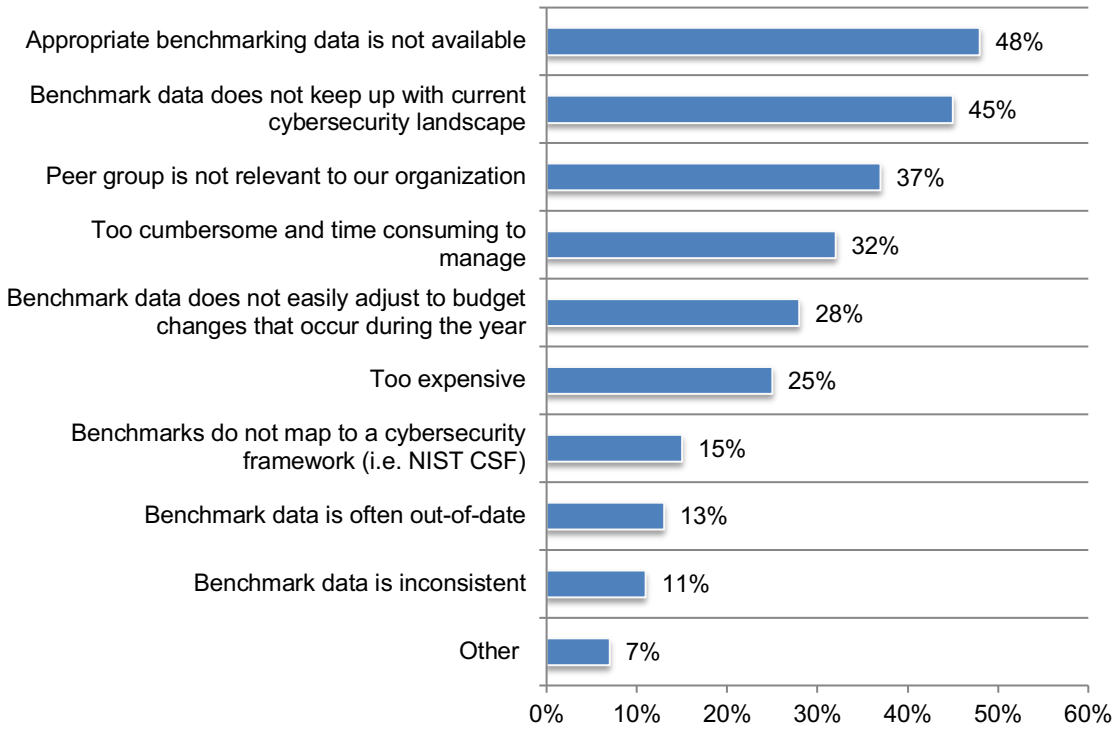
Benchmarking improves cybersecurity program decision making. 43 percent of respondents say their organizations are benchmarking their cybersecurity program against their peers. According to Figure 2, the primary value is to make better, data-driven decisions (53 percent of respondents). This is followed by demonstrating the effectiveness of benchmarking program investments (48 percent of respondents) and educating peers and others on the importance of cybersecurity (40 percent of respondents).

Figure 2. Why does your organization benchmark its cybersecurity program against its peers?
More than one response permitted



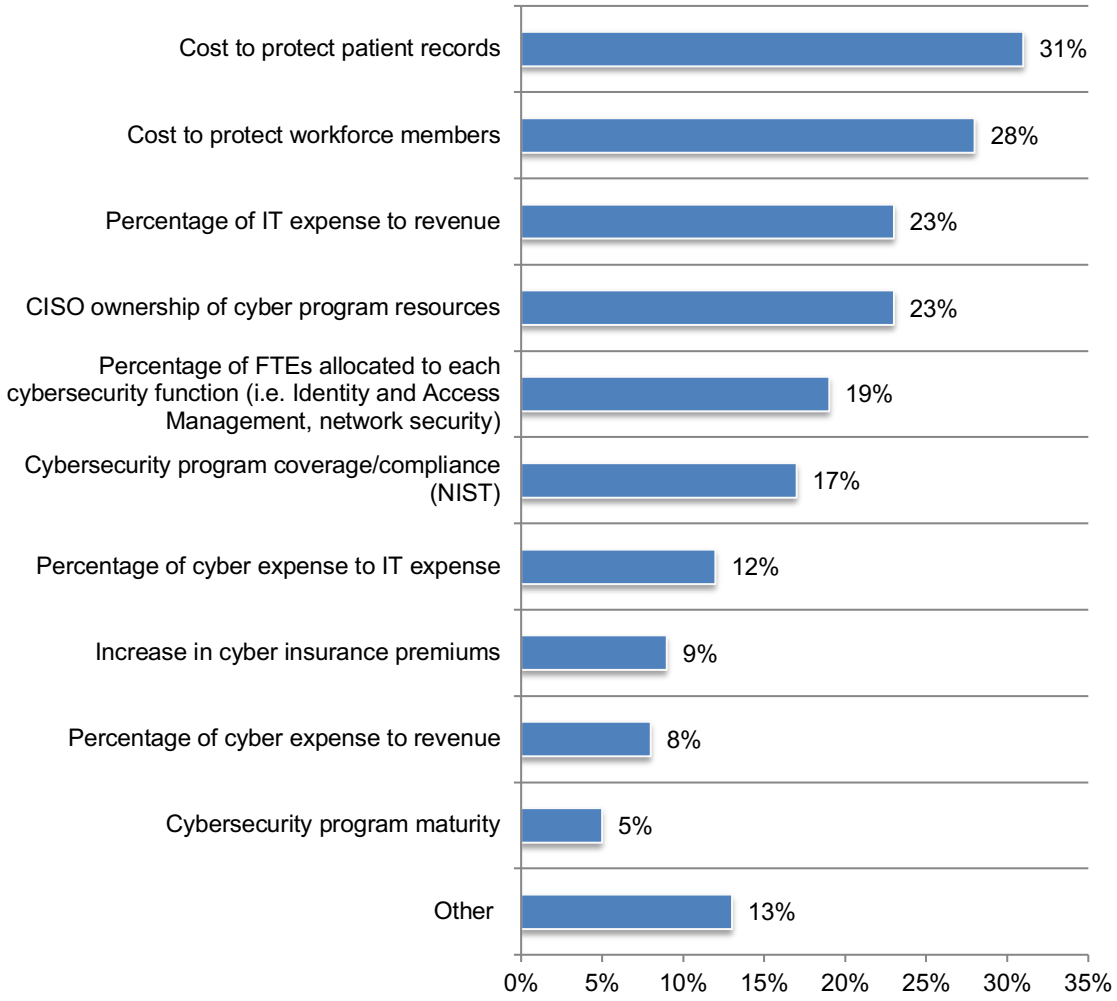
Issues with data discourage organizations from benchmarking their cybersecurity programs. Fifty-seven percent of respondents do not benchmark their cybersecurity programs against their peers. The primary reasons are: not having appropriate benchmarking data, and the benchmark data does not keep up with the current cybersecurity landscape.

Figure 3. If your organization doesn't benchmark its cybersecurity program, why?
More than one response permitted



Cost measures are most often used to determine the effectiveness of cybersecurity programs. According to Figure 4, 31 percent of respondents say their organizations measure the cost to protect patient records and to protect workforce members.

Figure 4. What benchmarking metrics does your organization use?
More than one response permitted

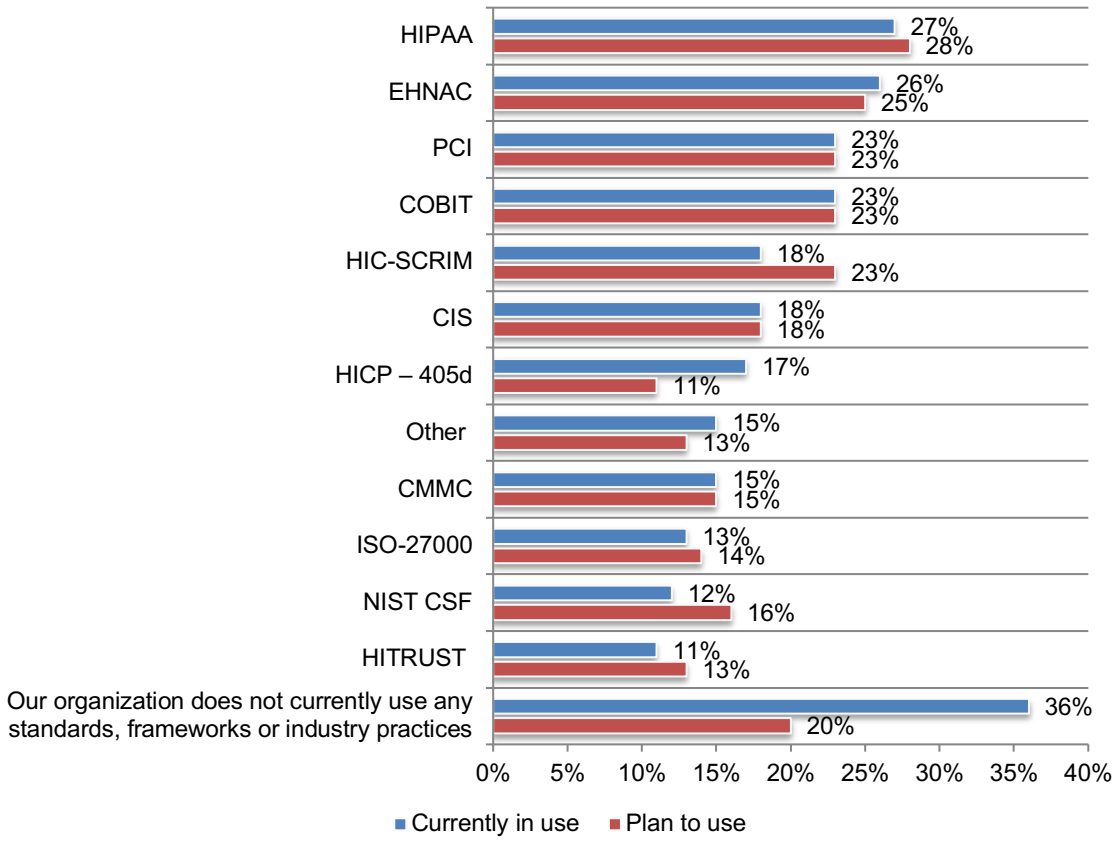


In the next 12 to 24 months, more organizations will use standards, frameworks or industry practices as the basis for their cybersecurity program. Figure 5 presents these standards, frameworks or industry practices and how their usage will change in the future.

Currently, 36 percent of respondents do not use standards, frameworks or industry practices. However, over the next 12 to 24 months only 20 percent of respondents say their organizations will not use them.

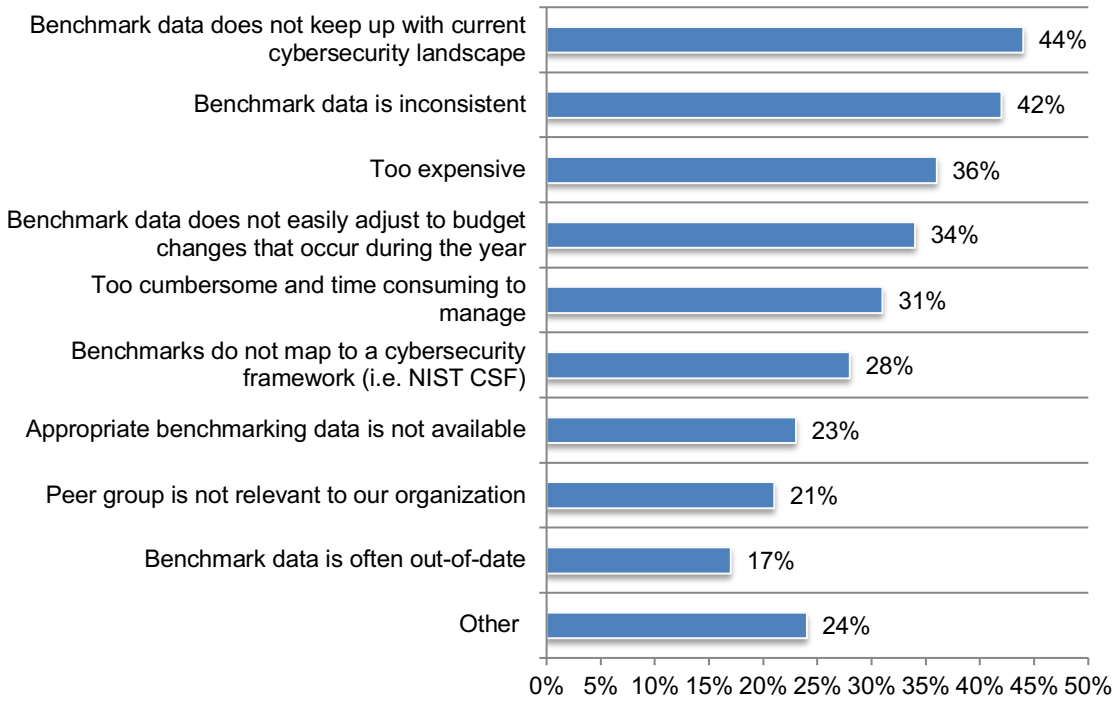
Certain standards, frameworks or industry practices will increase in usage. These include HIC-SCRIM (from 18 percent of respondents to 23 percent of respondents) and NIST CSF (12 percent of respondents to 16 percent of respondents). According to the research, the adoption of HICP – 405d will decline (17 percent of respondents to 11 percent of respondents).

Figure 5. What are the top standards, frameworks or industry practices currently used or plan to use as the basis for its cybersecurity program?
More than one response permitted



Not having current or consistent benchmark data are the top challenges to having an effective cybersecurity benchmarking data. As shown in Figure 6, 44 percent of respondents say benchmark data does not keep up with the current cybersecurity landscape and 42 percent of respondents say the data is inconsistent. The cost of benchmarking the cybersecurity program does not seem to be a significant challenge. Only 36 percent of respondents say benchmarking is too expensive and only 34 percent of respondents say benchmark data does not easily adjust to budget changes.

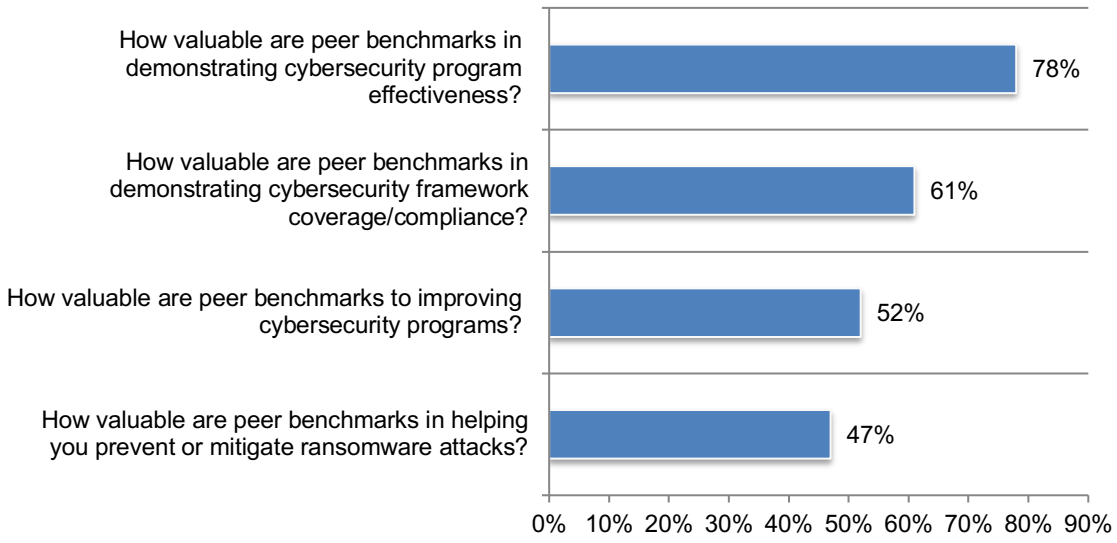
Figure 6. What are the primary challenges to having an effective cybersecurity benchmarking program?
Three responses permitted



Peer benchmarking is very valuable in demonstrating cybersecurity program effectiveness. In addition to enabling organizations to allocate the appropriate resources to reduce cyberattacks, benchmarking is valuable in demonstrating cybersecurity program effectiveness.

Respondents were asked to rate the value of different aspects of peer benchmarking cybersecurity programs on a scale from 1 = not valuable to 10 = very valuable. Figure 7 presents the 7+ responses on the 10-point scale. Most organizations find peer benchmarking valuable in demonstrating cybersecurity program effectiveness. Also valuable is the ability to demonstrate cybersecurity framework coverage/compliance (61 percent of respondents) and improving cybersecurity programs (52 percent of respondents). Forty-seven percent of respondents say benchmarking helps prevent or mitigate ransomware attacks.

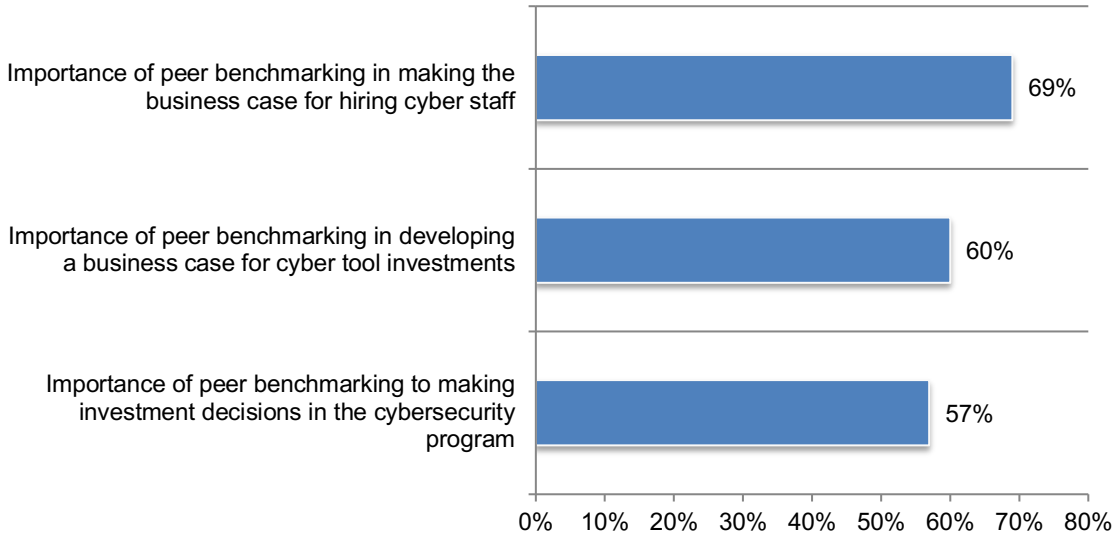
Figure 7. The value of benchmarking cybersecurity programs
On a scale from 1 = not valuable to 10 = very valuable, 7+ responses shown



Peer benchmarking makes organizations more effective in investment and resource allocation, especially when making the case to hire cyber staff. Benchmarks are valuable in improving organizations' ability to hire more in-house expertise, which is critical to having an effective cybersecurity program.

Respondents were asked to rate the importance of benchmarking to investments in staff and technologies on a scale from 1 = not important to 10 = very important. Figure 8 shows the 7+ responses on a scale from 1 = not important to 10 = very important. 69 percent of respondents say benchmarking is critical in making the business case for hiring cyber staff, 60 percent of respondents say it is important in developing a business case for cyber tool investments and 57 percent of respondents say it is important to making investment decisions.

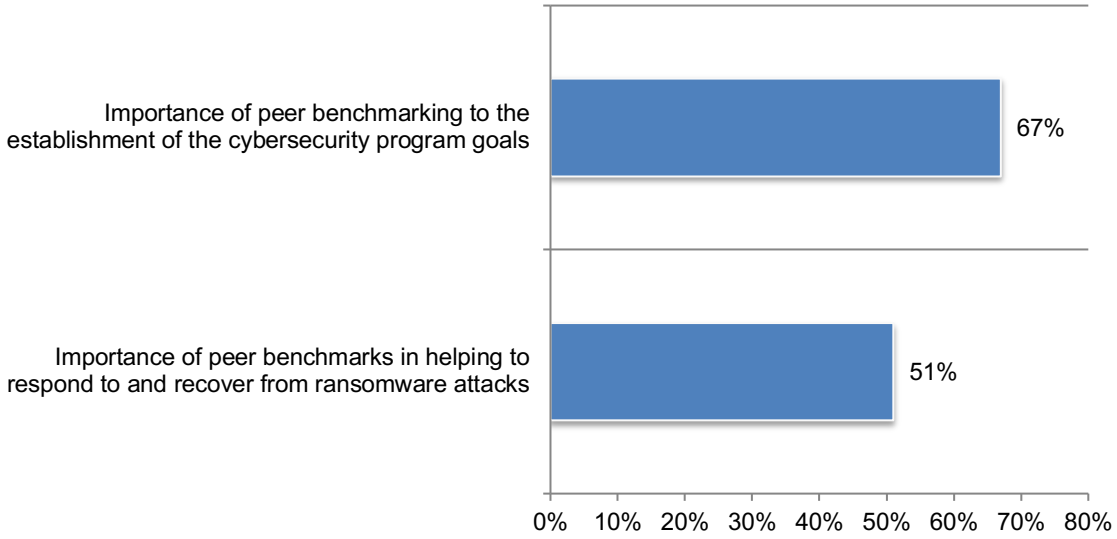
Figure 8. The importance of benchmarking to investment and resource allocation
On a scale from 1 = not important to 10 = very important, 7+ responses shown



Peer benchmarking is most important in establishing cybersecurity program goals. Respondents were asked to rate the importance of benchmarking to establishing goals and reducing risks on a scale of 1 = not important to 10 = very important. Figure 9 presents the 7+ responses on the 10-point scale.

While 47 percent say benchmarking is effective in preventing ransomware attacks, 51 percent of respondents say peer benchmarking is important to responding and recovering from ransomware attacks. As shown, benchmarking is also very important to establishing cybersecurity goals (67 percent of respondents).

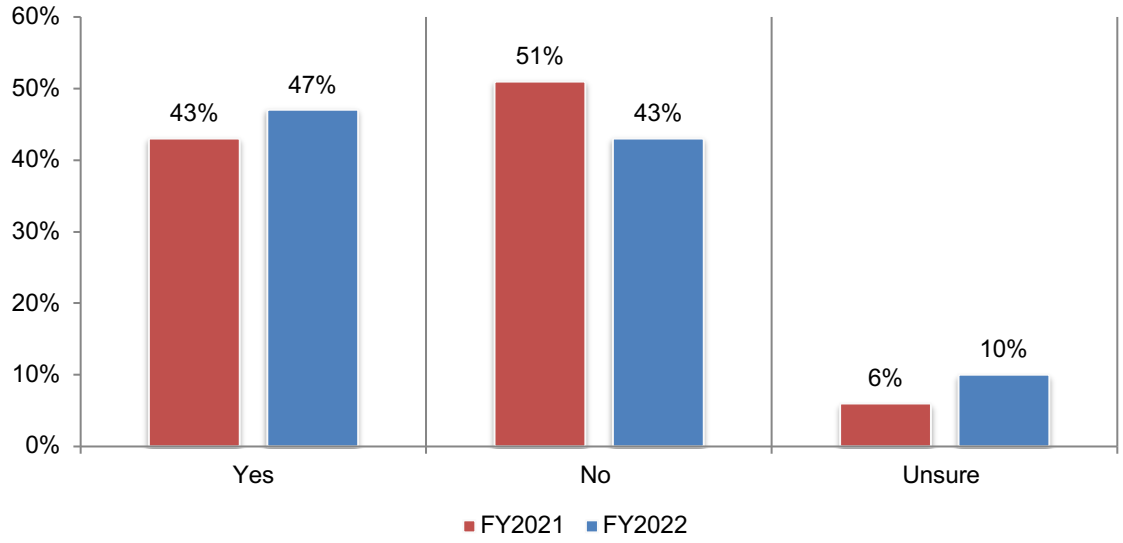
Figure 9. The importance of benchmarking to achieve cybersecurity program goals and respond to and recover from ransomware attacks
On a scale from 1 = not important to 10 = very important, 7+ responses shown



2.2 The two-year trend in the rise of ransomware in healthcare

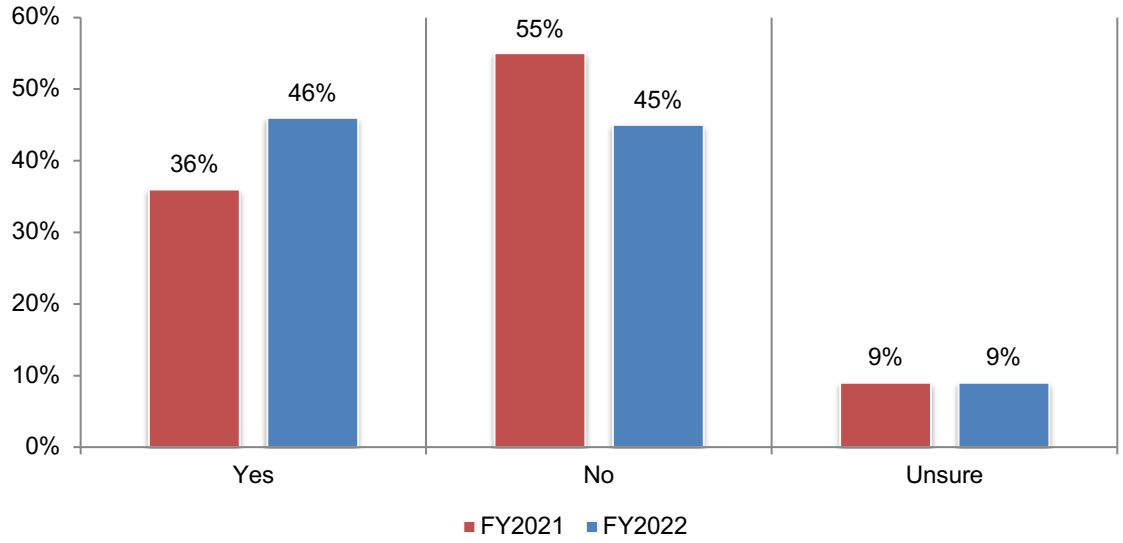
Ransomware attacks are on the rise. As shown in Figure 10, 47 percent of respondents say their organizations experienced a ransomware attack. However, 10 percent of respondents are unsure. In the past two years, 93 percent of these organizations experienced an average of at least one (65 percent) or between two and five (28 percent) ransomware attacks.

Figure 10. Did your organization ever experience a ransomware attack?



Third-party ransomware attacks increase significantly. Of the 47 percent of respondents who reported a ransomware attack, 46 percent of respondents say it was caused by a third party. This finding indicates the importance of having policies and processes in place to assess third parties, identify and remediate third party security gaps, and quickly respond and recover from a third-party ransomware attack.

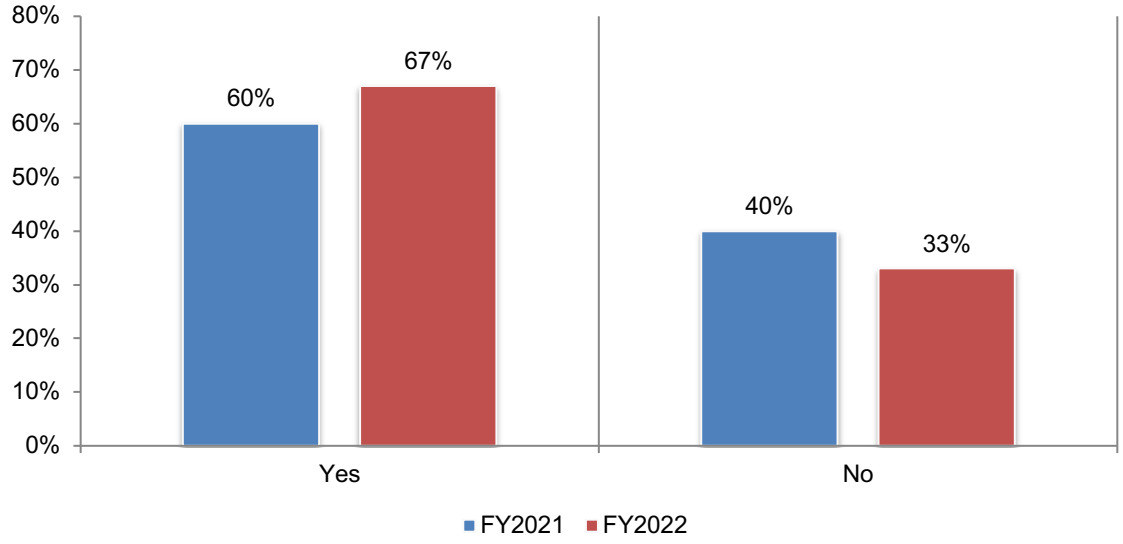
Figure 11. Were any of these caused by a third party?



More organizations are paying the ransom and organizations are not reducing the duration of these incidents. 67 percent of respondents say their organizations paid the ransom, an increase from 60 percent of respondents.

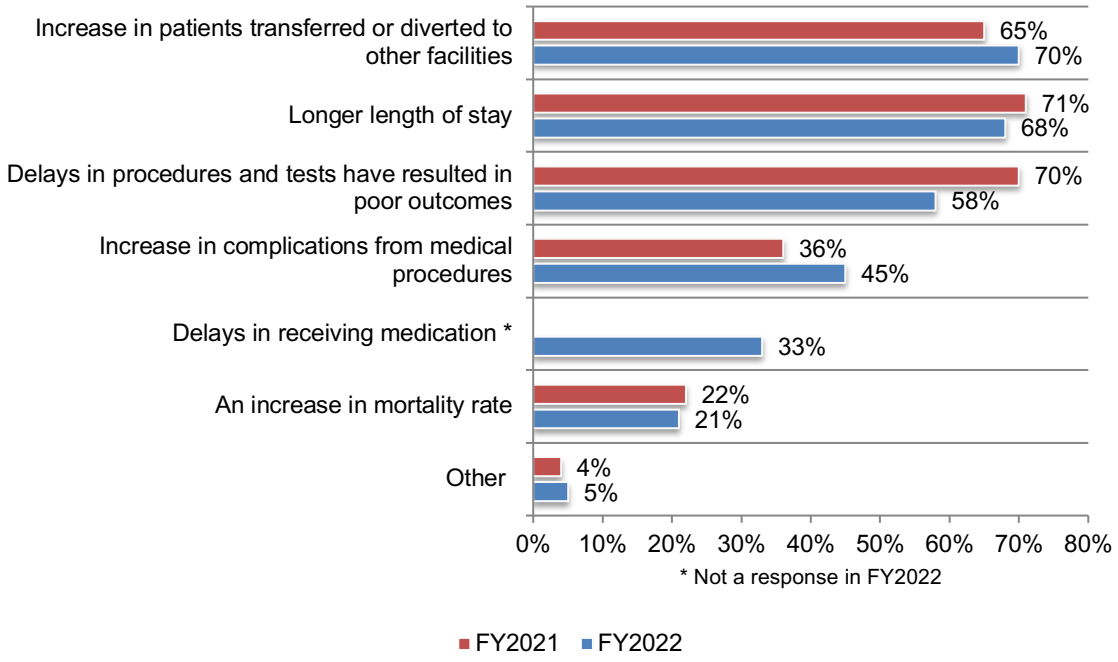
Ransomware payments increased from an average of $282,675 in 2021 to $352,541 in 2022. The average duration of the ransomware disruption stayed about the same from 39 days to 35 days.

Figure 12. Did your organization pay the ransom?



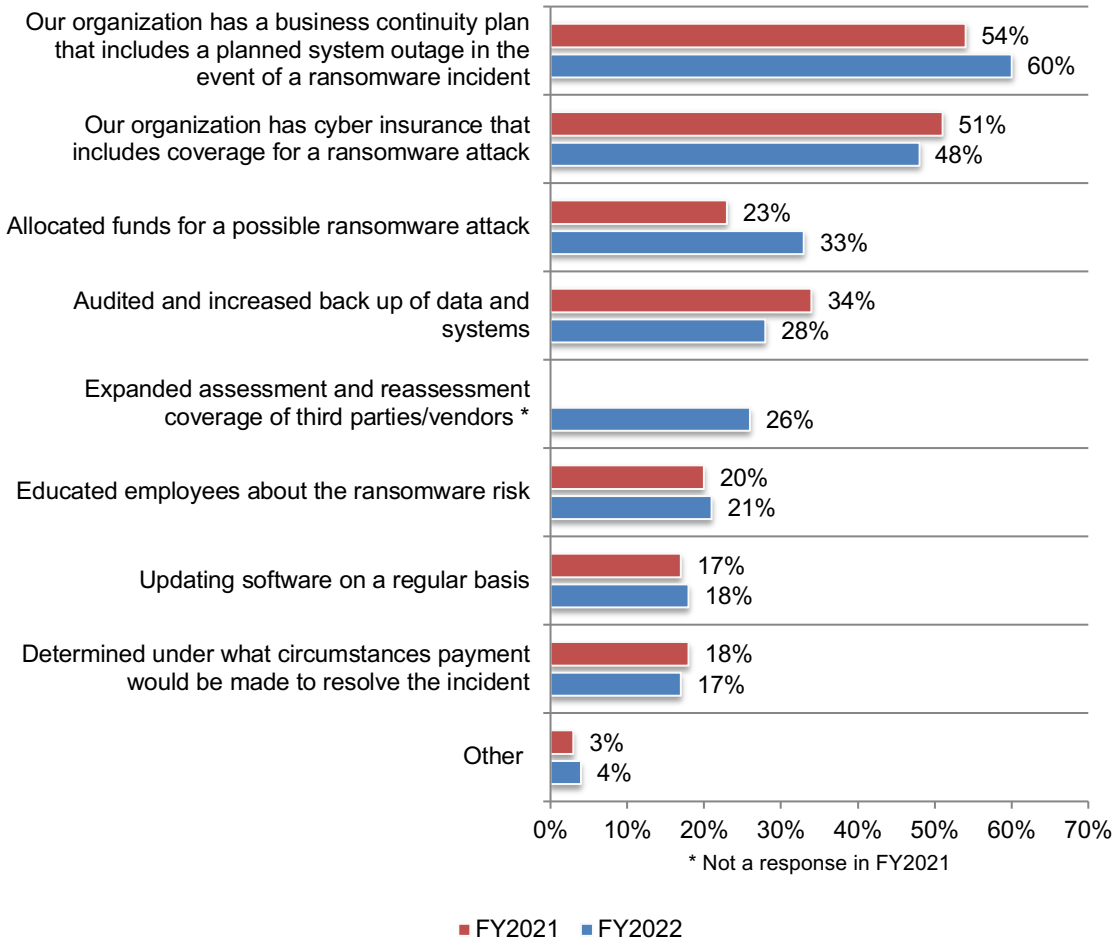
Ransomware attacks result in a significant increase in complications from medical procedures. More than half of respondents in organizations that had a ransomware attack, 53 percent, say it resulted in a disruption to patient care, a significant increase from 45 percent in 2021. As shown in Figure 13, more respondents in 2022 believe ransomware attacks result in an increase in complications from medical procedures than in 2021 (36 percent of respondents to 45 percent of respondents). The most adverse event is the increase in patients transferred or diverted to other facilities.

Figure 13. What impact did the ransomware attack have on patient care?
More than one response permitted



Business continuity plans are increasingly the most important step to preparing for a ransomware attack. Figure 14 lists the steps taken to prepare for a ransomware attack. In 2022, 60 percent of respondents say their organization has a business continuity plan that includes a planned system outage in the event of a ransomware incident, an increase from 54 percent of respondents in 2021. More organizations are allocating funds for a possible ransomware incident, an increase from 23 percent of respondents to 33 percent of respondents in this year's research.

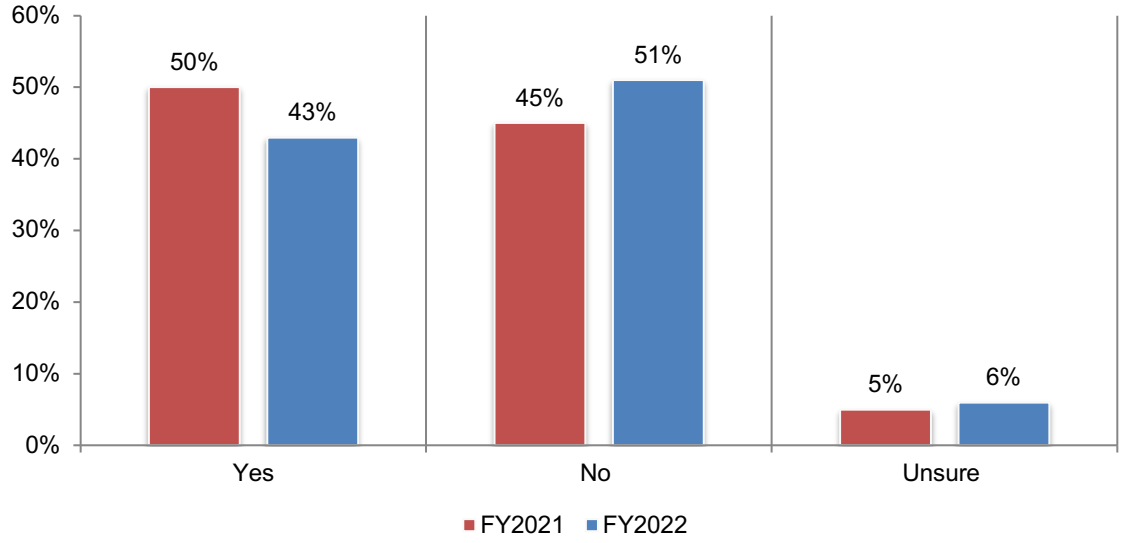
Figure 14. Have you taken the following steps to prepare for a ransomware attack?
More than one response permitted



2.3 Third-party risk management program assessment

Budgets for risk management programs have increased since 2021. According to Figure 15, since 2021, the percentage of organizations that have a formal budget has declined from 50 percent of respondents to 43 percent of respondents. However, those organizations with a formal budget on average are allocating more funds to the vendor risk management and investment in automation products in the upcoming fiscal year. In 2021, the budget was $890,000 and increased to $945,100 in this year's research.

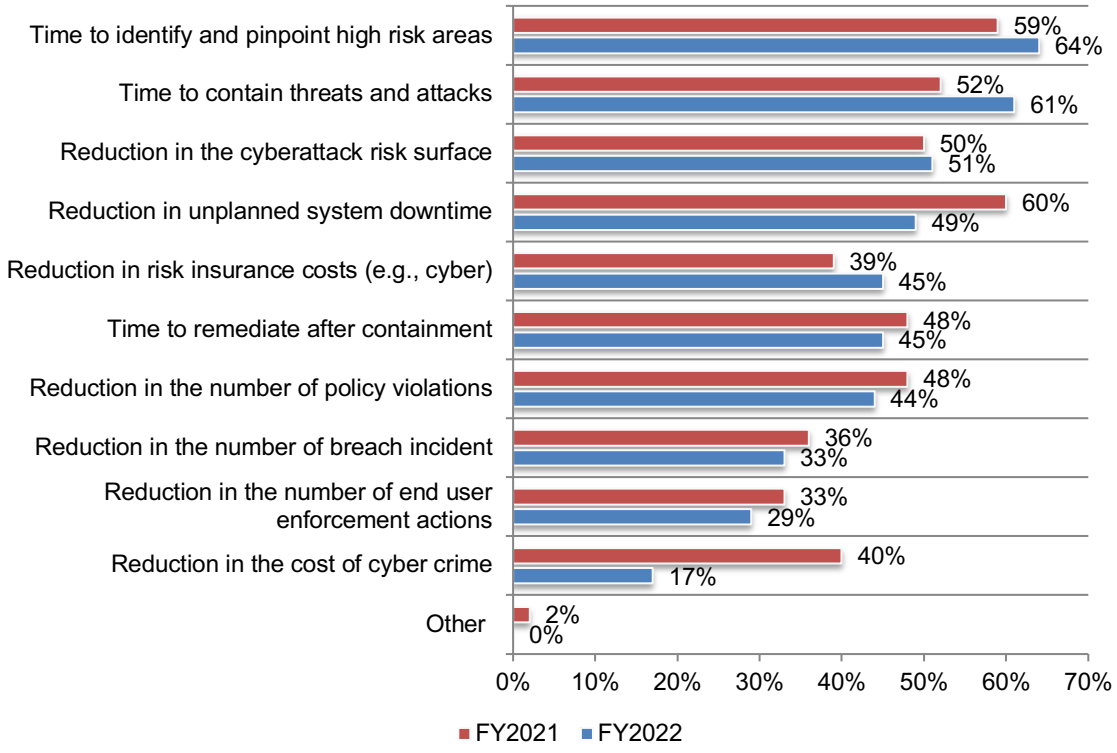
Figure 15. Does your organization have a formal budget for vendor risk management?



The most frequently used metrics to determine the effectiveness of third-party risk program efforts are the time it takes to find high risk areas and contain threats and attacks. Forty-six percent of respondents say their organizations measure the effectiveness of their third-party risk program efforts.

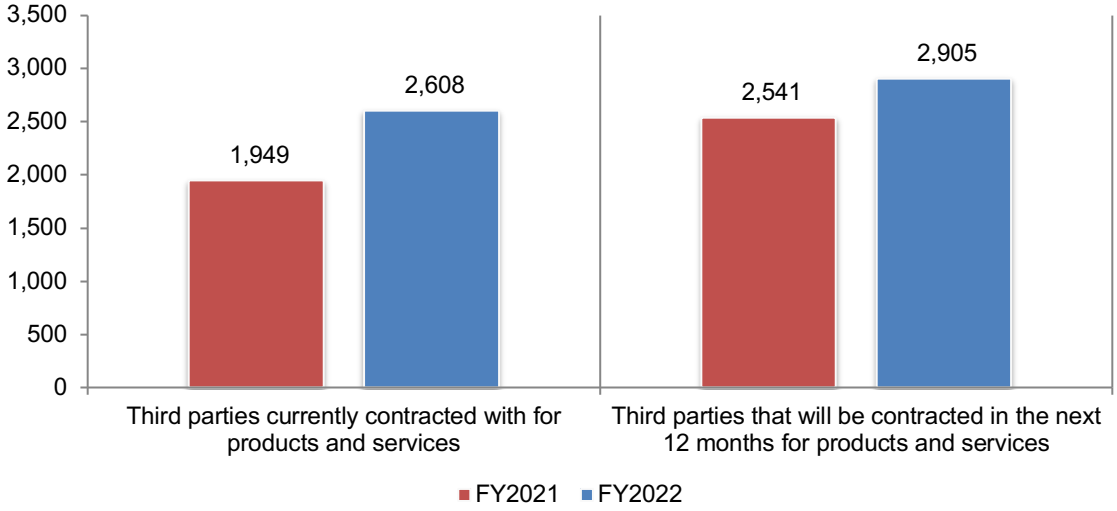
Of these respondents, 64 percent say they measure the time to identify and pinpoint high risk areas, an increase from 59 percent of respondents. Sixty-one percent of respondents track the time to contain threats and attacks, an increase from 52 percent to 61 percent in this year's study. Reduction in unplanned system downtime decreased from 60 percent of respondents to 49 percent and reduction in the cost of cyber crime declined from 40 percent to 17 percent of respondents.

Figure 16. What metrics are used to determine the effectiveness of its third-party risk program efforts?
More than one response permitted



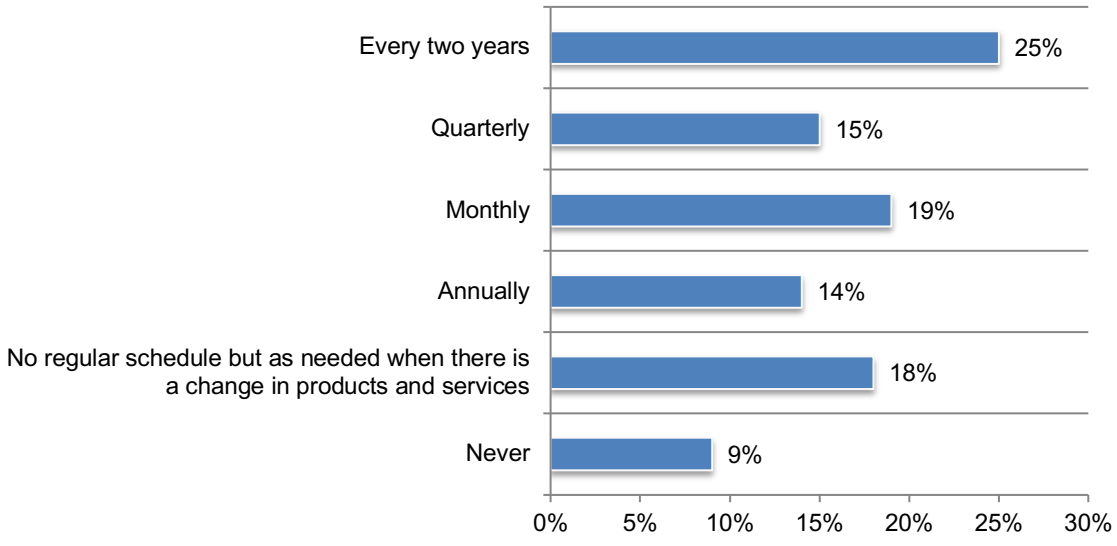
The average number of organizations' third parties is steadily increasing making it critical to have an effective vendor risk management program. As shown in Figure 17, the average number of current third parties increased from 1,949 in 2021 to 2,608 in this year's study. In the next 12 months, the average number will increase from an average of 2,541 to 2,905.

Figure 17. Trends in the number of organizations' third parties
Extrapolated values presented.



Less than half (48 percent) of respondents say their organizations are currently or will in the future assess the security and privacy of their third parties' products and services. In addition, these assessments are conducted infrequently. As shown in Figure 18, of these respondents, 43 percent say their organizations conduct an assessment every two years (25 percent) or there is no regular schedule and is based on a change in products and services (18 percent).

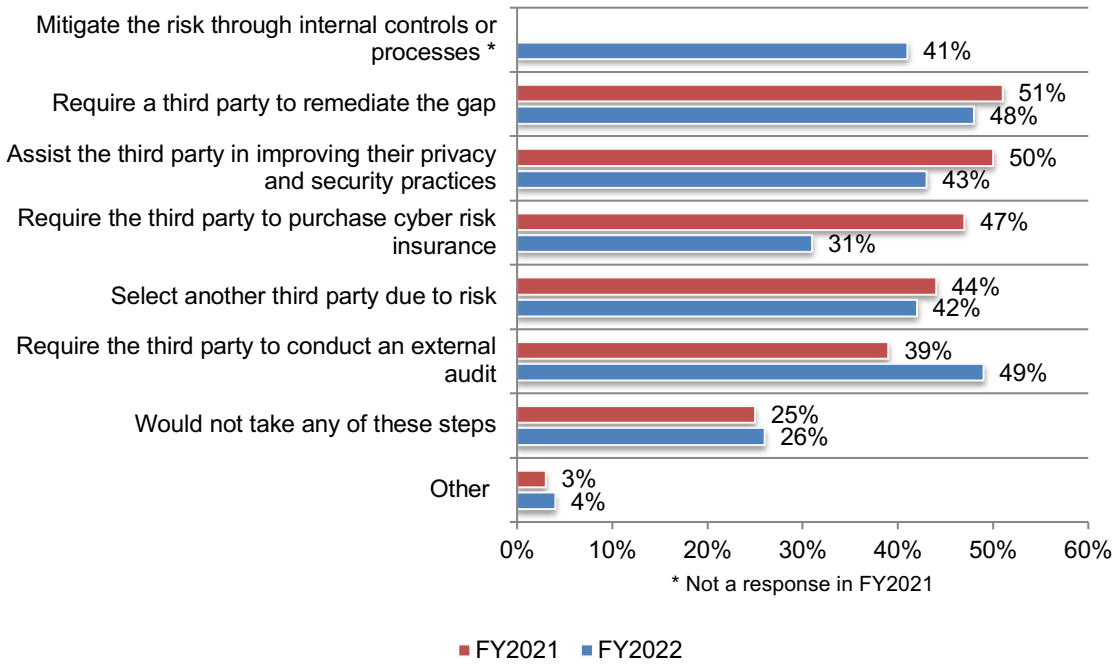
Figure 18. How often are re-assessments of these third parties conducted?



When third party's privacy and security policies appear to be inadequate, external audits are called for. According to Figure 19, 74 percent of respondents say their organizations would take steps to close the gaps in their third-party's privacy and security policies when discovered.

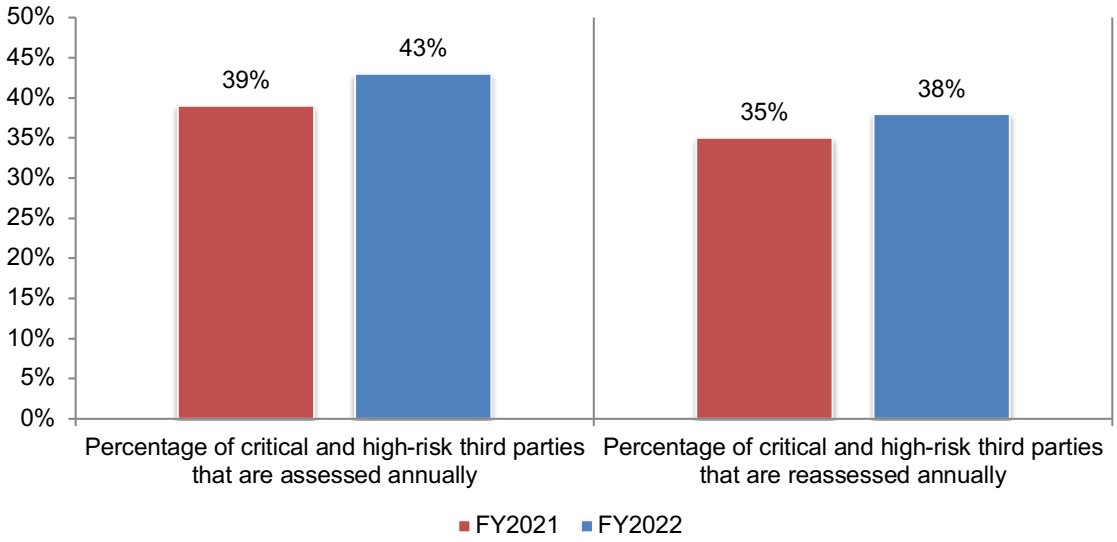
Since 2021, more organizations are requiring the third party to conduct an external audit, an increase from 39 percent to 49 percent. Fewer organizations are requiring third parties to purchase cyber risk insurance (31 percent) and assisting them in improving their privacy and security practices.

Figure 19. What steps would be taken if gaps in third-party's privacy and security policies were discovered?
More than one response permitted



Most organizations would assess the risks of all vendors and products/services if they had the resources and money. Seventy-three percent of respondents would assess the risks of **all** vendors and products/services regardless of a pre-assessment label of critical, high, medium or low, an increase from 65 percent of respondents in 2021. However, as shown in Figure 20, only an average of 43 percent of critical and high-risk third parties are assessed annually and only an average of 38 percent are reassessed annually.

Figure 20. The percentage of organization's critical and high-risk third parties that are assessed and reassessed annually
Extrapolated values presented



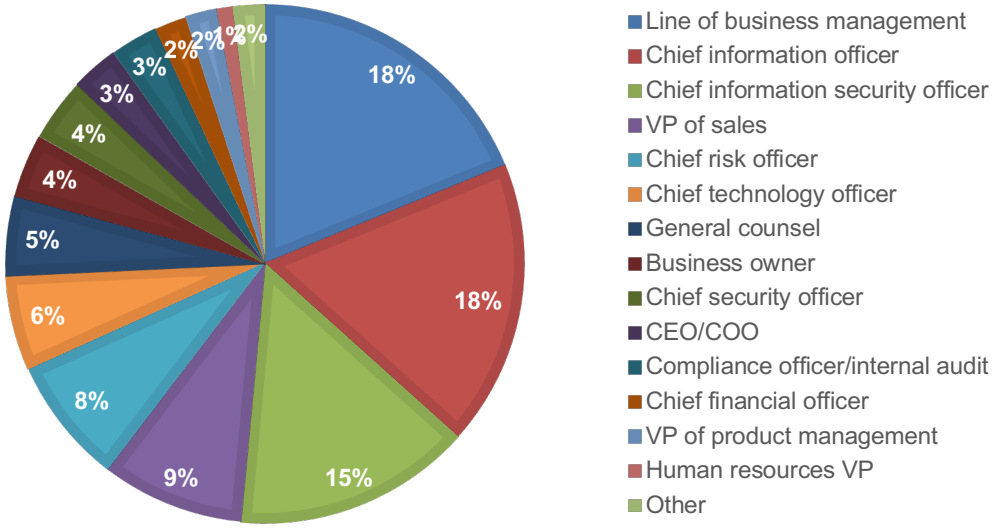
Part 3. Methodology

A sampling frame of 17,550 IT and IT security professionals in HDOs were selected as participants to this survey. Table 1 shows 649 total returns. Screening and reliability checks required the removal of 70 surveys. Our final sample consisted of 579 surveys or a 3.3 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,550	100.0%
Total returns	649	3.7%
Rejected or screened surveys	70	0.4%
Final sample	579	3.3%

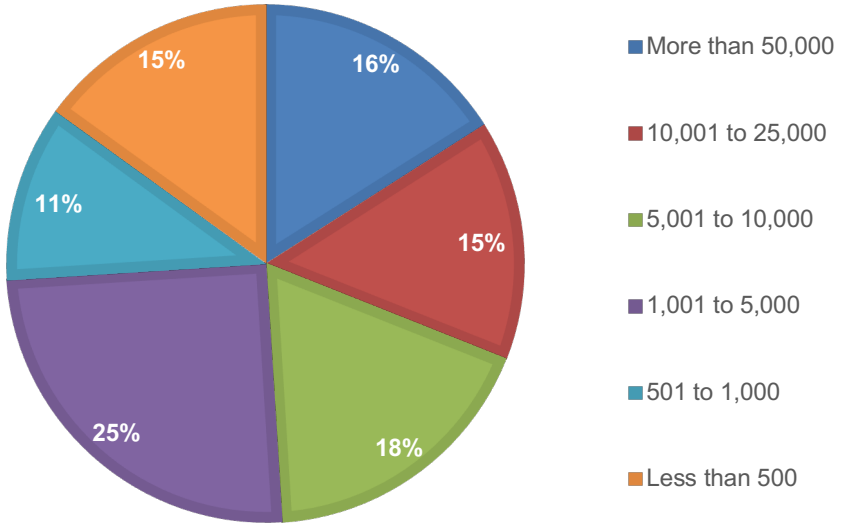
Pie chart 1 reports the primary person the respondent's report to within their organization. Eighteen percent of respondents report to the line of business manager and another 18 percent report to the chief information officer. This is followed by 15 percent of respondents that report directly to the chief information security officer and 9 percent of respondents that report to the VP of sales.

Pie chart 1. Primary Person reported to within the organization



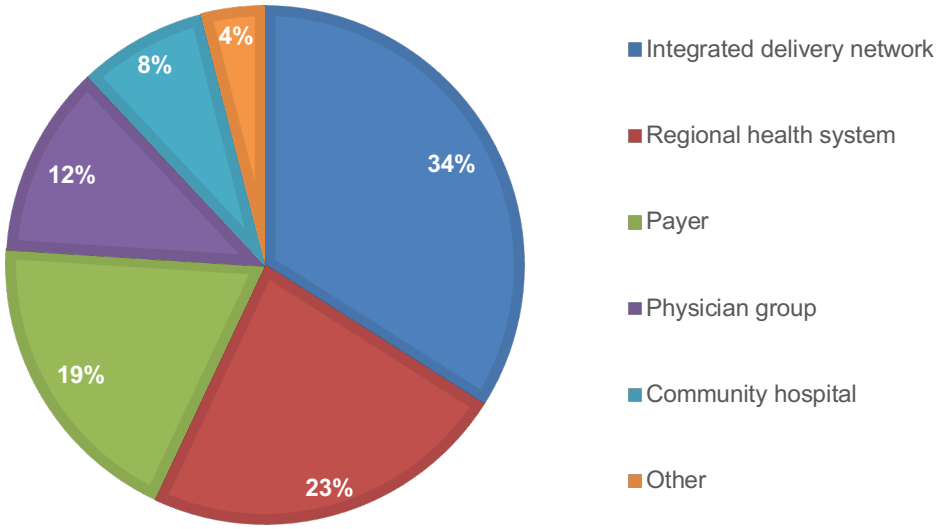
Almost half (49 percent) of respondents are from HDO organizations with an employee headcount of more than 5,000 employees, as shown in Pie Chart 2.

Pie Chart 2. The number of employees within the respondent's HDO organization



Pie Chart 3 identifies the type of organizations in which the respondents are located. Thirty-four percent of respondents are employed in organizations that are integrated delivery networks. This is followed by regional health systems (23 percent of respondents), payer (19 percent of respondents), and physician groups (12 percent of respondents).

Pie Chart 3. 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 October 2022.

Survey response	FY2022	FY2021
Total sampling frame	17,550	16,540
Total returned surveys	649	664
Rejected surveys	70	67
Final survey	579	597
Response rate	3.3%	3.6%

Part 1. Screening questions

S1. Is your healthcare organization an HDO as defined above?	FY2022	FY2021
Yes	100%	100%
No (stop)	0%	0%
Total	100%	100%

S2. How familiar are you with your organization's cybersecurity and risk management program?	FY2022	FY2021
Very familiar	36%	44%
Familiar	43%	38%
Somewhat familiar	21%	18%
No (stop)	0%	0%
Total	100%	100%

S3. What best describes your position? Select only one choice.	FY2022
Clinical/biomedical engineering leadership	14%
Clinical/biomedical engineering staff	21%
Executive (CEO, COO, CFO, etc.)	6%
IT administration	8%
IT leadership (CIO, CTO)	7%
IT operations	4%
IT security leadership (CISO)	2%
Medical informatics leadership (CMIO, VP, etc.)	0%
Operations or facilities leadership	7%
Risk or compliance leadership	4%
Risk or compliance staff	3%
None of the above (Stop)	24%
Total	100%

Part 2. Cybersecurity program benchmarks

Q1. Does your organization benchmark its cybersecurity program against its peers?	FY2022
Yes	43%
No	57%
Total	100%

Q2. If no, why doesn't your organization benchmark its cybersecurity program against its peers? Please select **all that apply**.	FY2022
Appropriate benchmarking data is not available	48%
Benchmark data does not easily adjust to budget changes that occur during the year	28%
Benchmark data does not keep up with current cybersecurity landscape	45%
Benchmark data is inconsistent	11%
Benchmark data is often out-of-date	13%
Benchmarks do not map to a cybersecurity framework (i.e. NIST CSF)	15%
Peer group is not relevant to our organization	37%
Too cumbersome and time consuming to manage	32%
Too expensive	25%
Other	7%
Total	261%

Q3. How many peers are in your organization's cohort or group?	FY2022
1	19%
2 to 3	21%
4 to 6	13%
7 to 10	16%
11 to 20	14%
21 to 50	9%
50+	8%
Total	100%
Extrapolated value	10.52

Q4. What benchmarking metrics does your organization use? Please select all that apply.	FY2022
CISO ownership of cyber program resources	23%
Cost to protect patient records	31%
Cost to protect workforce members	28%
Cybersecurity program coverage/compliance (NIST)	17%
Cybersecurity program maturity	5%
Increase in cyber insurance premiums	9%
Percentage of cyber expense to IT expense	12%
Percentage of cyber expense to revenue	8%
Percentage of FTEs allocated to each cybersecurity function (i.e. Identity and Access Management, network security)	19%
Percentage of IT expense to revenue	23%
Other	13%
Total	188%

Q5. What sources does your organization use for its cybersecurity benchmarks? Please select all that apply.	FY2022
American Hospital Association (AHA)	34%
Big 4 Accounting firms (Deloitte, PwC)	23%
Consulting firms	31%
H-ISAC	12%
HIMSS	13%
IT analysts (Gartner, Forrester)	20%
Law firms	23%
Proprietary peer group	17%
Self-managed ISAO	11%
Other	9%
Total	193%

Q6. Which industry standards, frameworks or industry practices does your organization **currently use** as the basis for its cybersecurity program? Please select all that apply.	FY2022
CIS	18%
CMMC	15%
COBIT	23%
EHNAC	26%
HIC-SCRIM	18%
HICP – 405d	17%
HIPAA	27%
HITRUST	11%
ISO-27000	13%
NIST CSF	12%
PCI	23%
Our organization **does not currently use** any standards, frameworks or industry practices	36%
Other	15%
Total	254%

Q7. In the next 12 to 24 months, which industry standards, frameworks or industry practices does your organization **plan to use** as the basis for its cybersecurity program? Please select all that apply.	FY2022
CIS	18%
CMMC	15%
COBIT	23%
EHNAC	25%
HIC-SCRIM	23%
HICP – 405d	11%
HIPAA	28%
HITRUST	13%
ISO-27000	14%
NISTCSF	16%
PCI	23%
Our organization **does not plan to use** any standards, frameworks or industry practices	20%
Other	13%
Total	242%

Q8. Why does your organization benchmark its cybersecurity program against its peers? Please select the **top three** reasons.	FY2022
Demonstrate duty of care standard with regulators (i.e. OCR)	39%
Demonstrate effectiveness of benchmarking program investments	48%
Educate peers and others on the importance of cybersecurity	40%
Gain support and resources from senior leadership and board of directors	27%
Improve cybersecurity program and roadmap planning	32%
Improve cybersecurity program investment decisions	24%
Make better, data-driven decisions	53%
Provide evidence of program maturity to cyber insurers	29%
Other	8%
Total	300%

Q9. What are the primary **challenges** to having an effective cybersecurity benchmarking program? Please select the **top three** reasons.	FY2022
Appropriate benchmarking data is not available	23%
Benchmark data does not easily adjust to budget changes that occur during the year	34%
Benchmark data does not keep up with current cybersecurity landscape	44%
Benchmark data is inconsistent	42%
Benchmark data is often out-of-date	17%
Benchmarks do not map to a cybersecurity framework (i.e. NIST CSF)	28%
Peer group is not relevant to our organization	21%
Too cumbersome and time consuming to manage	31%
Too expensive	36%
Other	24%
Total	300%

Q10. What is your organization's budget for its **2022** benchmarking program?	FY2022
$2,500 to $5,000	5%
$5,001 to $10,000	9%
$10,001 to $20,000	12%
$20,001 to $30,000	23%
$30,001 to $50,000	31%
$50,001 to $100,00	15%
More than $100,000	5%
Total	100%
Average	$ 38,200

Q11. What is your organization's budget for its **2023** benchmarking program?	FY2022
$2,500 to $5,000	2%
$5,001 to $10,000	3%
$10,001 to $20,000	19%
$20,001 to $30,000	19%
$30,001 to $50,000	35%
$50,001 to $100,00	17%
More than $100,000	5%
Total	100%
Average	$ 40,815

For the following questions, please use the 10-point scale from 1 = not valuable to 10 = very valuable

Q12a. How valuable are peer benchmarks to improving cybersecurity programs?	FY2022
1 or 2	6%
3 or 4	8%
5 or 6	34%
7 or 8	34%
9 or 10	18%
Total	100%
Extrapolated value	6.50

Q12b. How valuable are peer benchmarks to getting the right level of investment and resources for your organization's cybersecurity program?	FY2022
1 or 2	0%
3 or 4	6%
5 or 6	34%
7 or 8	34%
9 or 10	26%
Total	100%
Extrapolated value	7.10

Q12c. How valuable are peer benchmarks in demonstrating cybersecurity program effectiveness?	FY2022
1 or 2	3%
3 or 4	4%
5 or 6	15%
7 or 8	25%
9 or 10	53%
Total	100%
Extrapolated value	7.92

Q12d. How valuable are peer benchmarks in demonstrating cybersecurity framework coverage/compliance?	FY2022
1 or 2	8%
3 or 4	7%
5 or 6	24%
7 or 8	25%
9 or 10	36%
Total	100%
Extrapolated value	6.98

Q12e. How valuable are peer benchmarks in helping you prevent or mitigate ransomware attacks?	FY2022
1 or 2	13%
3 or 4	12%
5 or 6	28%
7 or 8	15%
9 or 10	32%
Total	100%
Extrapolated value	6.32

For the following questions, please use the 10-point scale from 1 = not important to 10 = very important below each question.

13a. How important is peer benchmarking to the establishment of your organization's cybersecurity program goals?	FY2022
1 or 2	6%
3 or 4	12%
5 or 6	15%
7 or 8	25%
9 or 10	42%
Total	100%
Extrapolated value	7.20

13b. How important is peer benchmarking to making investment decisions in your organization's cybersecurity program?	FY2022
1 or 2	11%
3 or 4	12%
5 or 6	20%
7 or 8	23%
9 or 10	34%
Total	100%
Extrapolated value	6.64

13c. How important is peer benchmarking to developing a business case for cyber tool investments?	FY2022
1 or 2	0%
3 or 4	6%
5 or 6	34%
7 or 8	23%
9 or 10	37%
Total	100%
Extrapolated value	7.32

13d. How important is peer benchmarking to making the business case for hiring cyber staff?	FY2022
1 or 2	6%
3 or 4	12%
5 or 6	13%
7 or 8	35%
9 or 10	34%
Total	100%
Extrapolated value	7.08

Q13e. How important are peer benchmarks in helping you respond to and recover from ransomware attacks?	FY2022
1 or 2	6%
3 or 4	11%
5 or 6	32%
7 or 8	20%
9 or 10	31%
Total	100%
Extrapolated value	6.68

Part 3. Third-party risk management program assessment

Q14a. Does your organization measure the effectiveness of its third-party risk program efforts?	FY2022
Yes	44%
No	56%
Total	100%

Q14b. If yes, what metrics are used? Please select all that apply.	FY2022	FY2021
Time to identify and pinpoint high risk areas	64%	59%
Time to contain threats and attacks	61%	52%
Time to remediate after containment	45%	48%
Reduction in risk insurance costs (e.g., cyber)	45%	39%
Reduction in the cyberattack risk surface	51%	50%
Reduction in unplanned system downtime	49%	60%
Reduction in the number of policy violations	44%	48%
Reduction in the number of end user enforcement actions	29%	33%
Reduction in the number of breach incident	33%	36%
Reduction in the cost of cyber crime	17%	40%
Other (please specify)	0%	2%
Total	438%	481%

Q15. How many third parties does your organization currently contract with for products and services?	FY2022	FY2021
Less than 250	16%	13%
250 to 500	21%	23%
501 to 1,000	13%	11%
1,001 to 2,500	23%	26%
2,501 to 5,000	19%	20%
5,001 to 10,000	5%	5%
More than 10,000	3%	2%
Total	100%	100%
Extrapolated value	2,608	1,949

Q16. In the next 12 months, how many third parties will your organization contract with for products and services?	FY2022	FY2021
Less than 250	8%	16%
250 to 500	18%	17%
501 to 1,000	19%	23%
1,001 to 2,500	14%	12%
2,501 to 5,000	20%	13%
5,001 to 10,000	17%	15%
More than 10,000	4%	4%
Total	100%	100%
Extrapolated value	2,905	2,541

Q17a. What percentage of these third parties are or will be assessed for the security and privacy of their products and services?	FY2022
0%	0%
1% to 25%	13%
26% to 50%	16%
51% to 75%	27%
76% to 100%	32%
100%	12%
Total	100%
Extrapolated value	**48%**

Q17b. How often are re-assessments of these third parties conducted?	FY2022	FY2021
Real time		12%
Monthly	19%	12%
Quarterly	15%	8%
Annually	14%	15%
On demand		23%
Every two years	25%	
No regular schedule but as needed when there is a change in products and services	18%	30%
Never	9%	
Total	100%	100%

Q18. What steps would your organization take if gaps in a third-party's privacy and security practices/policies were discovered? Please select all that apply.	FY2022	FY2021
Assist the third party in improving their privacy and security practices	43%	50%
Mitigate the risk through internal controls or processes	41%	
Require a third party to remediate the gap	48%	51%
Require the third party to conduct an external audit	49%	39%
Require the third party to purchase cyber risk insurance	31%	47%
Select another third party due to risk	42%	44%
Would not take any of these steps	26%	25%
Other (please specify)	4%	3%
Total	284%	259%

Q19. Does your organization determine which third parties are critical and high-risk to its operations?	FY2022
Yes	46%
No	54%
Total	100%

Q20. Does your organization require critical and high-risk third parties to have an **internal** risk assessment even if they have a recent SOC2 certification?	FY2022	FY2021
Yes	52%	46%
No	48%	54%
Total	100%	100%
Q21. Does your organization require critical and high-risk third parties to have an **internal** risk assessment even if they have recent HITRUST certification?	FY2022	FY2021
Yes	52%	56%
No	48%	44%
Total	100%	100%

Q22. What is the percentage of your organization's critical and high-risk third parties that are **assessed** annually?	FY2022	FY2021
Zero	13%	11%
1% to 25%	37%	38%
26% to 50%	26%	27%
51% to 75%	12%	15%
76% to 100%	12%	9%
Total	100%	100%
Extrapolated value	**43%**	**39%**

Q23. What is the percentage of your organization's critical and high-risk third parties that are **reassessed** annually?	FY2022	FY2021
Zero	14%	15%
1% to 25%	39%	41%
26% to 50%	28%	27%
51% to 75%	12%	12%
76% to 100%	7%	5%
100%	100%	100%
Extrapolated value	**38%**	**35%**

Q24. If you had the resources and money, would your organization assess the risks of **all** its vendors and products/services, regardless of a pre-assessment label of critical, high, medium or low?	FY2022	FY2021
Yes	73%	65%
No	27%	35%
Total	100%	100%

Part 4. Impact of ransomware

Q25. Have you taken the following steps to prepare for a ransomware attack? Please select all that apply.	FY2022	FY2021
Allocated funds for a possible ransomware attack	33%	23%
Audited and increased back up of data and systems	28%	34%
Our organization has a business continuity plan that includes a planned system outage in the event of a ransomware incident	60%	54%
Our organization has cyber insurance that includes coverage for a ransomware attack	48%	51%
Determined under what circumstances payment would be made to resolve the incident	17%	18%
Educated employees about the ransomware risk	21%	20%
Expanded assessment and reassessment coverage of third parties/vendors	26%	
Updating software on a regular basis	18%	17%
Other	4%	3%
Total	255%	220%

Q26. Did your organization **ever** experience a ransomware attack?	FY2022	FY2021
Yes	47%	43%
No	43%	51%
Unsure	10%	6%
Total	100%	100%

Q27. In the past two years, how many ransomware incidents did your organization experience?	FY2022	FY2021
One	65%	67%
2 to 5	28%	31%
6 to 10	4%	2%
More than 10	3%	0%
Total	100%	100%

Q28. Were any of these caused by a third party?	FY2022	FY2021
Yes	46%	36%
No	45%	55%
Unsure	9%	9%
Total	100%	100%

Q29a. Did your organization pay the ransom?	FY2022	FY2021
Yes	67%	60%
No	33%	40%
Total	100%	100%

Q29b. If yes, in the past two years how much **total** ransom did your organization pay?	FY2022	FY2021
Less than $10,000	30%	25%
$10,000 to $25,000	19%	21%
$25,001 to $50,000	8%	12%
$50,001 to $75,000	5%	9%
$75,001 to $100,000	10%	11%
$100,001 to $250,000	7%	6%
$250,001 to $500,000	11%	8%
$500,001 to $1,000,000	6%	5%
$1,00,001 to $5,000,000	0%	1%
$5,00,001 to $10,000,000	3%	2%
More than $10,000,000	1%	0%
Total	100%	100%
Extrapolated Average (US$ Millions)	$ 352,541	$ 282,675

Q30. What was the duration of the ransomware disruption?	FY2022	FY2021
Less than 1 day	35%	40%
1 day to 7 days	26%	46%
8 days to 14 days	16%	7%
15 days to 30 days	5%	5%
More than 30 days		2%
30 days to 60 days	11%	
More than 60 days	7%	
Total	100%	100%
Extrapolated value (Days of elapsed time)	**35.40**	**39.43**

Q31a. Did the ransomware attack result in a disruption in patient care operations?	FY2022	FY2021
Yes	53%	45%
No	41%	50%
Unsure	6%	5%
Total	100%	100%

Q31b. If yes, what impact did the ransomware attack have on patient care? Please select all that apply.	FY2022	FY2021
An increase in mortality rate	21%	22%
Delays in procedures and tests have resulted in poor outcomes	58%	70%
Delays in receiving medication	33%	
Increase in complications from medical procedures	45%	36%
Increase in patients transferred or diverted to other facilities	70%	65%
Longer length of stay	68%	71%
Other	5%	4%
Total	300%	268%

Part 5. Risk ownership and budget

Q32. Who has overall responsibility for your organization's risk management approach or strategy? Please select only one choice.	FY2022	FY2021
Chief Risk Officer	5%	6%
Chief Information Officer	26%	35%
Chief Financial Officer	5%	3%
Chief Information Security Officer	25%	23%
Chief Privacy Officer	4%	2%
No one person has overall responsibility	31%	28%
Other	4%	3%
Total	100%	100%

Q33a. Does your organization have a formal budget for vendor risk management activities/program?	FY2022	FY2021
Yes	43%	50%
No	51%	45%
Unsure	6%	5%
Total	100%	100%

Q33b. If yes, how much will your organization allocate to investment in vendor risk management and automation products in the upcoming fiscal year?	FY2022	FY2021
Less than $250,000	25%	29%
Between $250,000 and $500,000	25%	21%
Between $500,000 and $1 million	26%	22%
Between $1 and $2 million	14%	21%
Between $2 and $5 million	9%	5%
More than $5 million	1%	2%
Total	100%	100%
Extrapolated value	945,100	$ 890,000

Part 6: Organizational characteristics

D1. Check the **Primary Person** you report to within the organization	FY2022	FY2021
CEO/COO	3%	3%
Business owner	4%	2%
Chief financial officer (CFO)	2%	2%
General counsel	5%	3%
Chief information officer (CIO)	18%	30%
Chief technology officer (CTO)	6%	5%
Chief risk officer (CRO)	8%	7%
Chief information security officer (CISO)	15%	19%
Compliance officer/internal audit	3%	2%
Human resources VP	1%	0%
Chief security officer (CSO)	4%	3%
Line of business (LOB) management	19%	18%
VP of sales	9%	2%
VP of product management	2%	3%
Other	1%	1%
Total	100%	100%

D2. How many employees are in your HDO organization?	FY2022	FY2021
Less than 500	15%	12%
501 to 1,000	11%	13%
1,001 to 5,000	25%	23%
5,001 to 10,000	18%	20%
10,001 to 25,000	15%	20%
More than 50,000	16%	12%
Total	100%	100%

D3. What is the type of the organization?	FY2022
Integrated delivery network (IDN)	34%
Regional health system	23%
Community hospital	8%
Physician group	12%
Payer	19%
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.