Ponemon INSTITUTE

The State of Supply Chain Risk in Healthcare

Healthcare Sector Coordinating Council

Independently conducted by Ponemon Institute LLC

Publication Date: January 2023

Ponemon INSTITUTE

The State of Supply Chain Risk in Healthcare

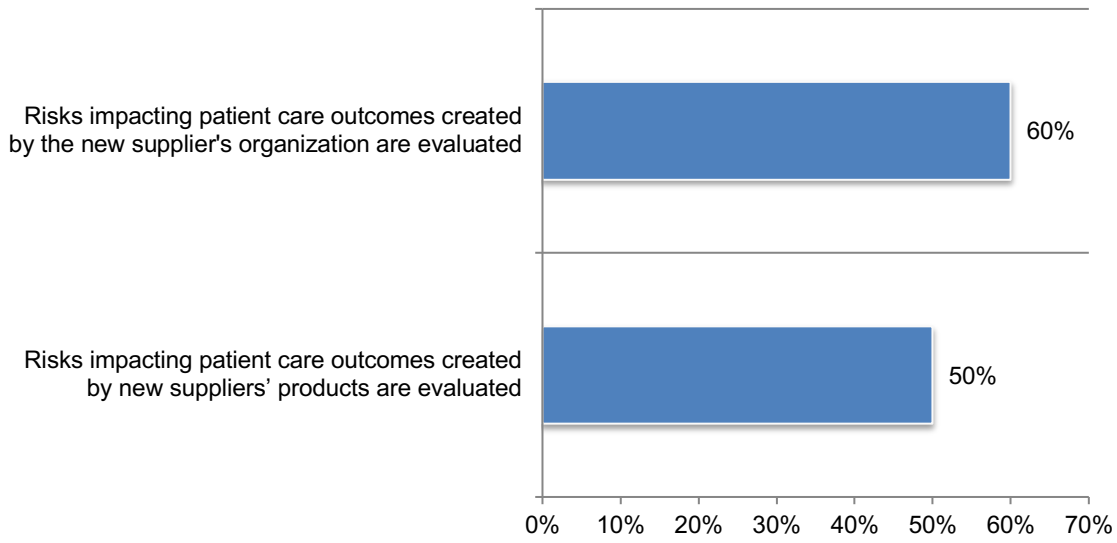
Ponemon Institute, January 2023

Part 1. Introduction

Ponemon Institute in collaboration with the Healthcare Sector Coordinating Council[1] conducted a study on the cybersecurity challenges facing the healthcare sector. More than 400 IT and IT security practitioners were surveyed who are involved in their organizations' supply chain risk management program (SCRM) and familiar with their cybersecurity plans or programs.

A key takeaway is that risks to patients caused by new suppliers are not being evaluated by many healthcare organizations. As shown in Figure 1**,** only half (50 percent) of respondents say their organizations evaluate the risks impacting patient care outcomes created by new suppliers' products. Sixty percent of respondents say new suppliers are evaluated to understand if there would be adverse patient outcomes created by these organizations. According to the research, pre-existing and legacy suppliers are more likely to be included in the organizational SCRM.

Figure 1. Does your organization evaluate the risks impacting patient care outcomes created by new suppliers?
Yes responses



The following findings reveal why the supply chain is vulnerable to a cyberattack.

Most organizations are in the dark about potential risks created by suppliers. Only 19 percent of respondents say their organizations have a complete inventory of their suppliers of physical goods, business-critical services and/or third-party information technology.

Business-critical suppliers are not regularly evaluated for their security practices. Forty-four percent of respondents say security evaluations are conducted of those suppliers who are business-critical on an ad-hoc basis (24 percent) or only when a security incident occurs (20 percent).

[1] The Healthcare and Public Sector Coordinating Council (HSCC) is a coalition of private-sector, critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public.

Most organizations are not assessing suppliers' software and technology. Only 43 percent of respondents say their SCRM program assesses the integrity/provenance of suppliers' software and technology. Forty-three of percent of respondent say their organizations will accept certifications such as PCI-DSS, ISO-27001 in lieu of the usual assessment/attestation process for suppliers.

Pre-existing suppliers and not new suppliers are more likely to be included in the scope of an organization's SCRM. Fifty-four percent of respondents say pre-existing suppliers that have been on-boarded before the establishment of the program are primarily included in the SCRM process. Only 46 percent of respondents say new suppliers are included.

Rarely are suppliers categorized based on their connectivity or network access to the healthcare organization. Only about half **(**53 percent of respondents) say their organizations categorize suppliers as part of the SCRM program. Of these, 43 percent of respondents say categorization is based on the nature of the products or services and 40 percent of respondents say it is based on the data shared with these suppliers. Only 10 percent of respondents say it is based on connectivity or network access.

There is a lack of integration between procurement and/or contracting departments and the SCRM process that could affect the ability of contracts to ensure the security of the supply chain. Only 41 percent of respondents say the procurement and/or contracting departments are integrated with their organization's SCRM process. Only 25 percent of respondents say their organizations always add supplier remediations into their contracts if needed.

The lack of standardized language in security contracts and supply chain issues is a deterrent to an effective SCRM program. In addition to the lack of standardized security contractual language in contracts (59 percent of respondents), healthcare SCRM programs are affected by problems with the supply chain. These problems include challenges identifying critical suppliers as the supplier relationship evolves over time (49 percent of respondents), lack of risk tiering of suppliers (49 percent of respondents) and lack of supplier incident or vulnerability notification (45 percent of respondents)

Healthcare organizations face the challenge of having the in-house expertise and senior leadership support needed to have a successful SCRM program. Respondents were asked to select the reasons for not having an effective SCRM program. Fifty-nine percent of respondents say it is the lack of in-house expertise and 55 percent of respondents say it is a lack of senior leadership support.

A lack of cooperation from suppliers and employees is the primary people-related impediment to a successful SCRM program. Fifty-four percent of respondents say the lack of co-operation from suppliers and 43 percent of respondents say it is the lack of inter-departmental co-operation that stands in the way of having an effective program.

Controlling the sprawl of software usage is the number one technology-related impediment to achieving an effective SCRM program. A barrier to an effective SCRM program is managing the sprawl of software usage (i.e., applications, components and cloud services), according to 55 percent of respondents. This is followed by the prompt delivery of software patches from third parties for required upgrades (45 percent of respondents) and the lack of visibility into the cloud environment used by third parties (44 percent of respondents).

To address the supply chain risks discussed above, healthcare organizations are making the following activities a priority.

Improvement of supply chain management is a priority. Sixty-seven percent of respondents say their organizations' top priority is implementing tools for supplier inventory management. This is followed by 63 percent of respondents who say their organizations will be implementing tools for assessment automation and 45 percent of respondents say their organizations will hire consultants for program and process definition.

Business goals for SCRM are the cost, product quality and the supply chain. Respondents were asked to identify the business goals driving the SCRM program. Fifty-nine percent of respondents say their organizations are prioritizing the impact to cost, performance, timing and availability of goods followed by 56 percent of respondents who say it is to minimize the impact of product quality. Almost half (48 percent of respondents) say it is to understand and improve cyber-resiliency of their supply chain.

Organizations are focused on tracking direct suppliers and products/services electronically (43 percent of respondents). Other top priorities are to have redundancy across critical suppliers and increase reassessments of suppliers, 36 percent and 32 percent of respondents respectively.

Part 2. Key findings

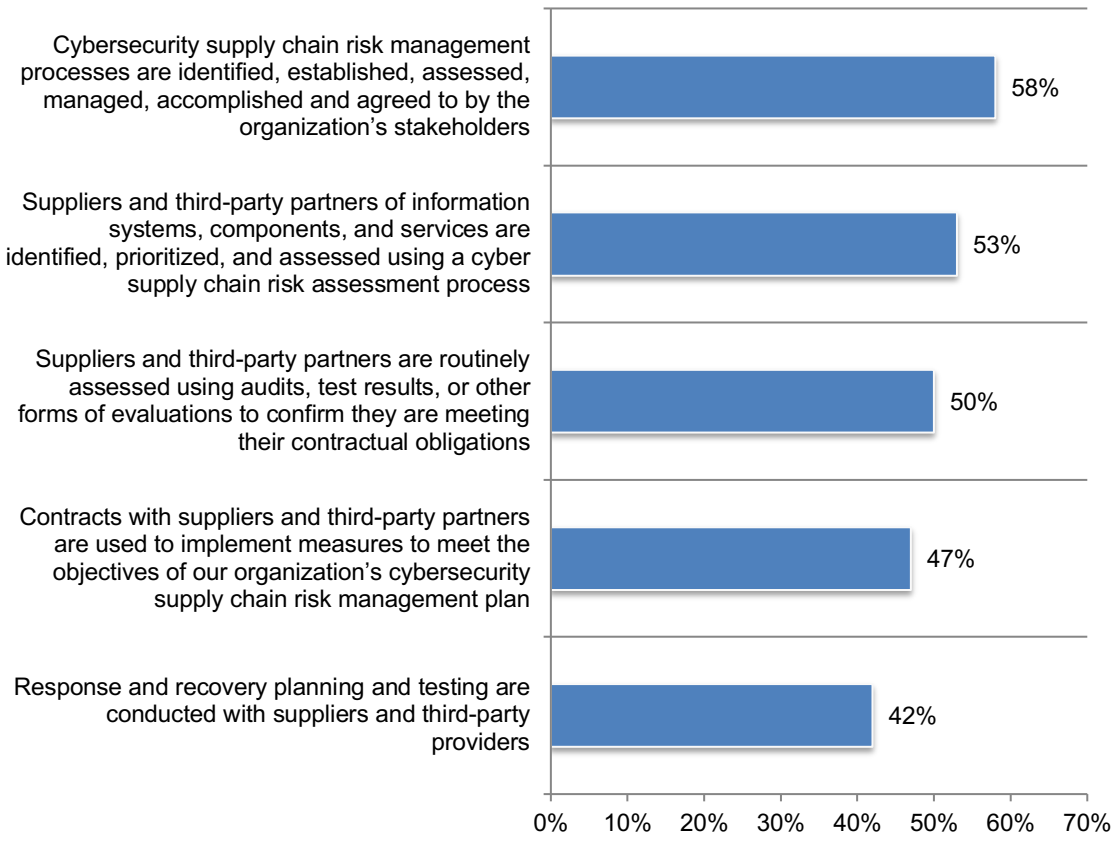
In this section, we present an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- The management of healthcare supplier risk
- Supplier risk governance practices
- The current and future state of SCRM healthcare programs

The management of supplier risk

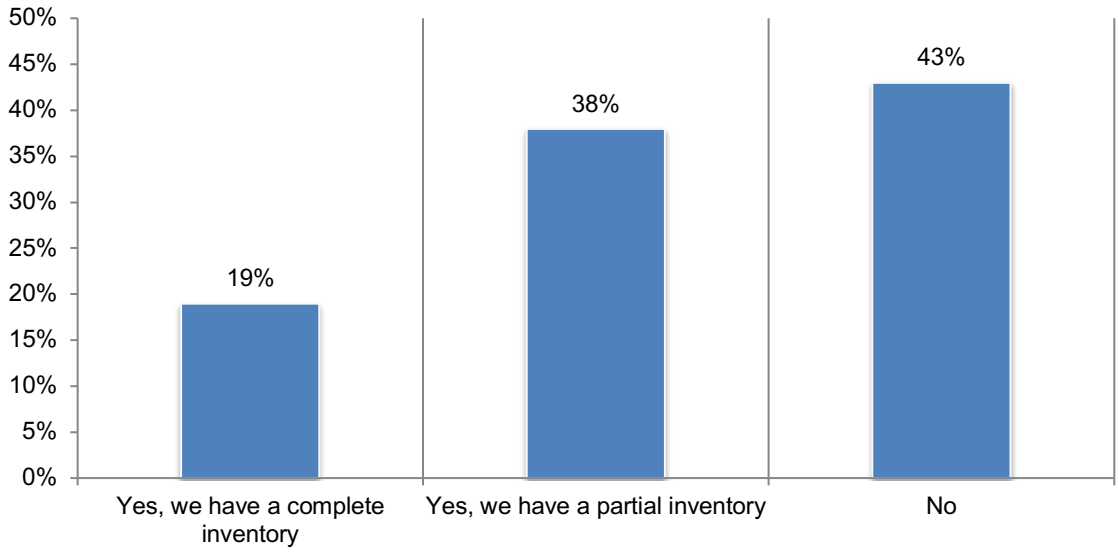
Many organizations do not have a mature approach to managing healthcare supplier risk. Figure 2 presents the various steps organizations are taking to manage healthcare supplier risk. As evidence of the lack of maturity, only 42 percent of respondents say their organizations have an incident response, recovery and testing plan with suppliers and third-party providers. The step most often taken is for the organizations' stakeholders to agree to cybersecurity supply chain risk management processes, according to 58 percent of respondents.

Figure 2. Perceptions about the management of healthcare supplier risk
Fully and partially accomplished responses presented The first bar should be established, assessed, **managed,** accomplished



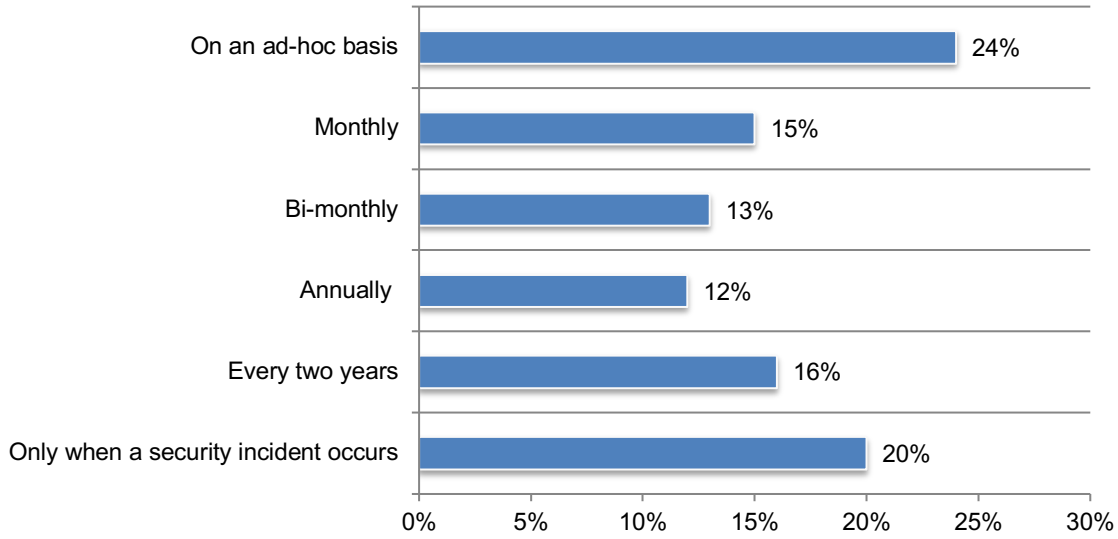
Most organizations are in the dark about potential risks created by suppliers. As shown in Figure 3, only 19 percent of respondents say their organizations have a complete inventory of their suppliers of physical goods, business-critical services and/or third-party information technology.

Figure 3. Does your organization maintain an updated, digital & centralized inventory of suppliers of physical goods, business-critical services and/or third-party information technology?



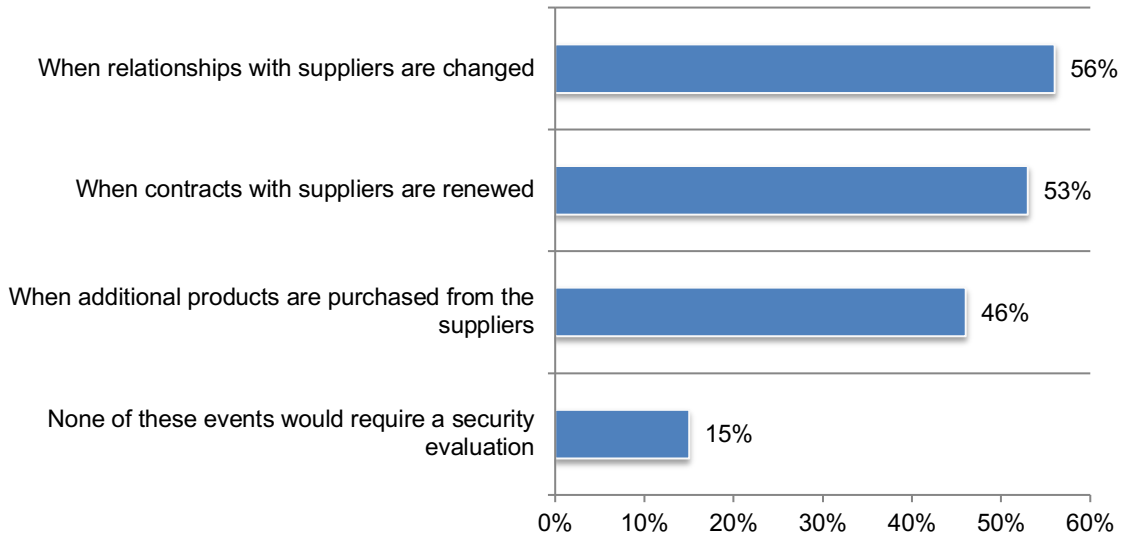
Business-critical suppliers are not regularly evaluated for their security practices. According to Figure 4, 44 percent of respondents say security evaluations are conducted of those suppliers who are business-critical on an ad-hoc basis (24 percent) or only when a security incident occurs (20 percent).

Figure 4. How often does your organization require a security evaluation of its business-critical suppliers?



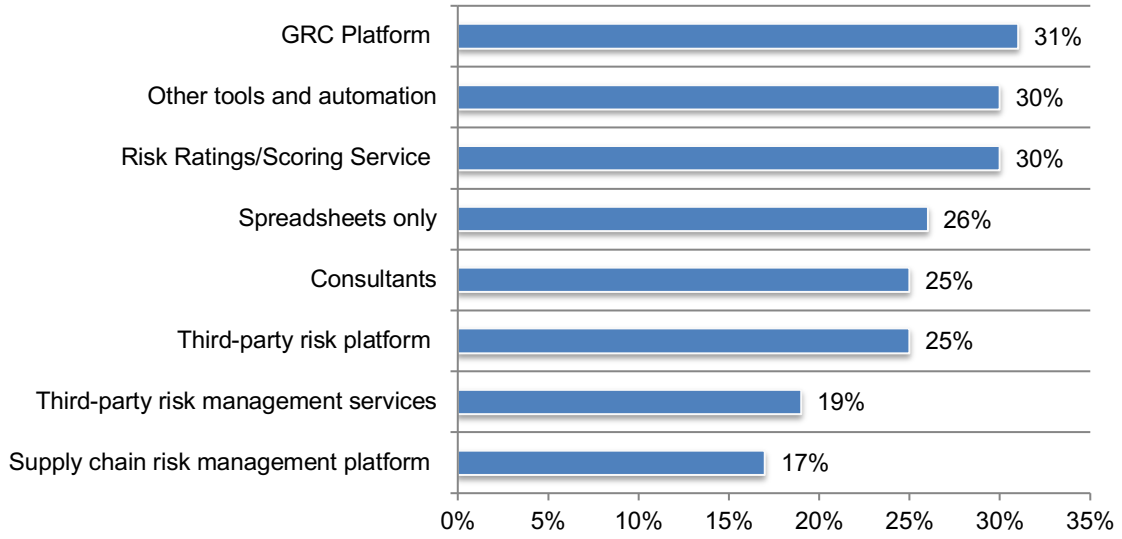
Changing relationships with business-critical suppliers and contract renewals are the two primary triggers for a security evaluation. As shown in Figure 5, 56 percent of respondents say their organizations evaluate suppliers' security practices and posture when the relationship changes and 53 percent of respondents say when contracts are renewed.

Figure 5. What events trigger a security evaluation of business-critical suppliers?
More than one response permitted



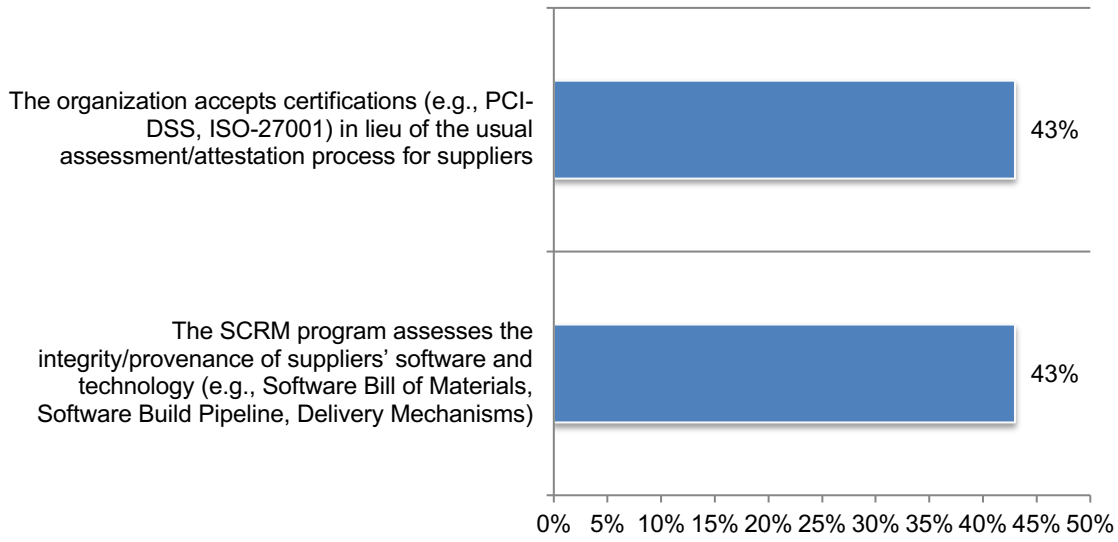
As discussed previously, most supplier evaluations are conducted on an ad-hoc basis or only when a security incident occurs. According to Figure 6, 31 percent of respondents say their organizations use a Governance Risk Compliance (GRC) platform followed by other tools and automation (30 percent).

Figure 6. What tools, technologies and services are used as part of your organization's supplier evaluation?
More than one response permitted



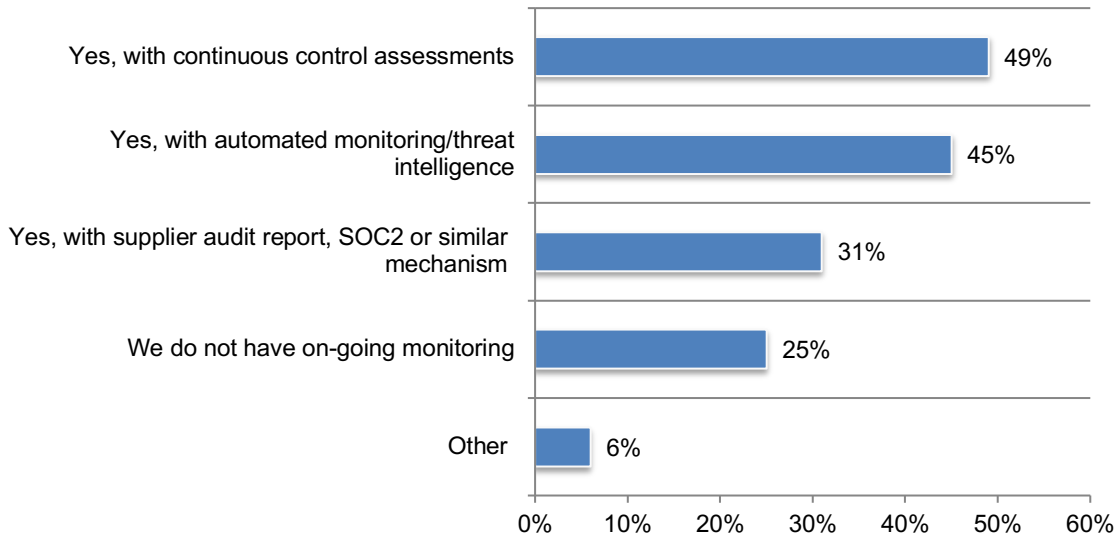
Most organizations are not assessing suppliers' software and technology. According to Figure 7, only 43 percent of respondents say their SCRM program assesses the integrity/provenance of suppliers' software and technology. However, only 43 percent will accept certifications such as PCI-DSS, ISO-27001 in lieu of the usual assessment/attestation process for suppliers.

Figure 7. Does the SCRM assess the suppliers' software and technology and/or accept certifications in lieu of the usual supplier assessment process?
Yes responses presented



Seventy-five percent of respondents have one or more approaches to monitoring suppliers as part of their SCRM process, according to Figure 8. The most often used are continuous control assessments (49 percent of respondents) and automated monitoring/threat intelligence (45 percent of respondents).

Figure 8. Does your organization have on-going monitoring as part of your SCRM process?
More than one response permitted



Supplier risk governance practices

Many organizations (51 percent) find frameworks or industry guides helpful in improving their SCRM program. Figure 9 presents a list of the most often used frameworks and industry guides to improve the security posture of the SCRM program. NIST is by far the most often used (54 percent of respondents).

Figure 9. Which frameworks or industry guides does your organization leverage in its SCRM?
More than one response permitted

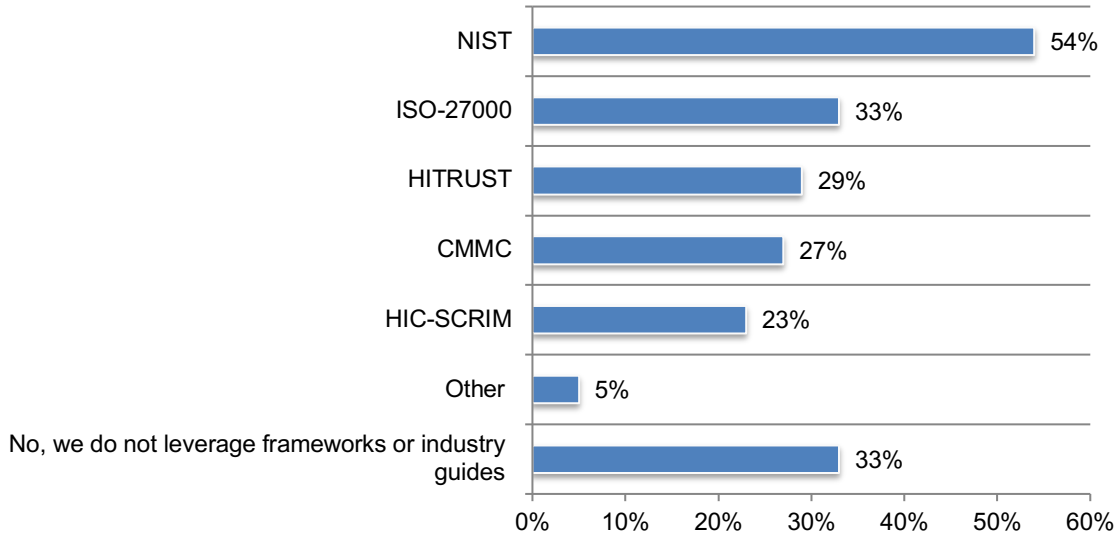
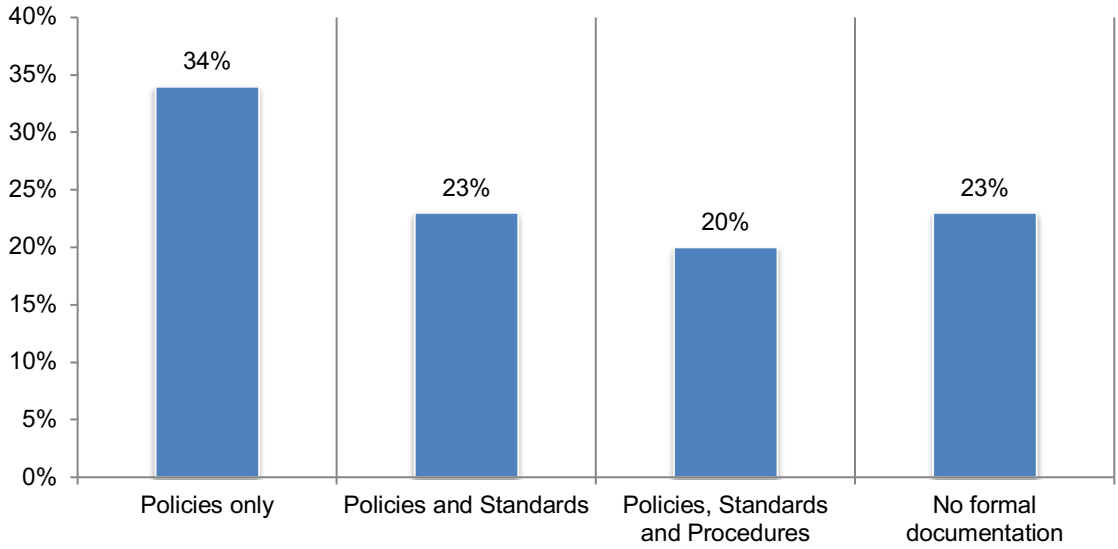


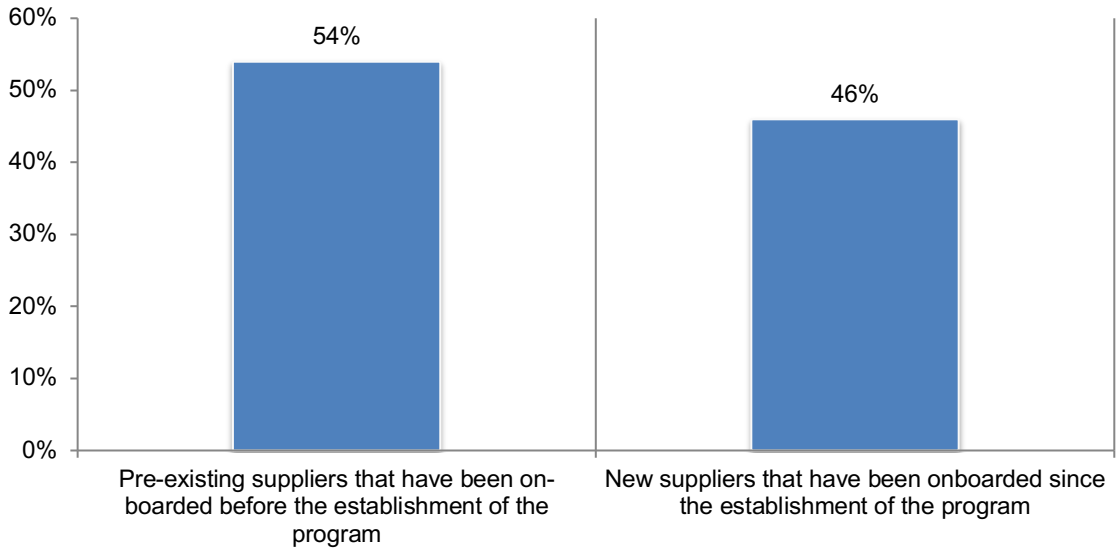
Figure 10 describes the formal documents for organizations' SCRM programs. Only 23 percent of respondents say their organizations have no formal documents. Thirty-four percent and 23 percent of respondents say policies and policies and standards are used, respectively.

Figure 10. What level of formal document does the SCRM program have?
Only one choice permitted



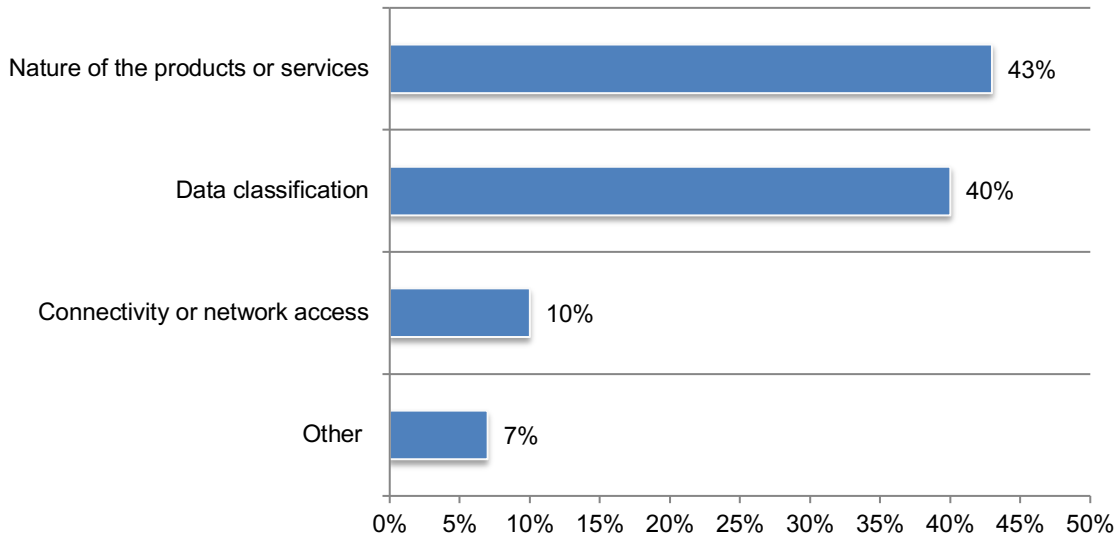
Pre-existing suppliers are more likely than new suppliers to be included in the scope of an organization's SCRM. According to Figure 11, 54 percent of respondents say pre-existing suppliers that have been on-boarded before the establishment of the program are primarily included. Only 46 percent of respondents say new suppliers are included.

Figure 11. Which of the following is included in the scope of your organization's SCRM program? Only one response permitted



Rarely are suppliers categorized based on their connectivity or network access to the healthcare organization. Fifty-three percent of respondents say their organizations categorize suppliers as part of the SCRM program. According to Figure 12, 43 percent of these respondents say the nature of the products or services and 40 percent of respondents say data shared with these suppliers are used to categorize suppliers. Only 10 percent of respondents say it is based on connectivity or network access to the healthcare organization.

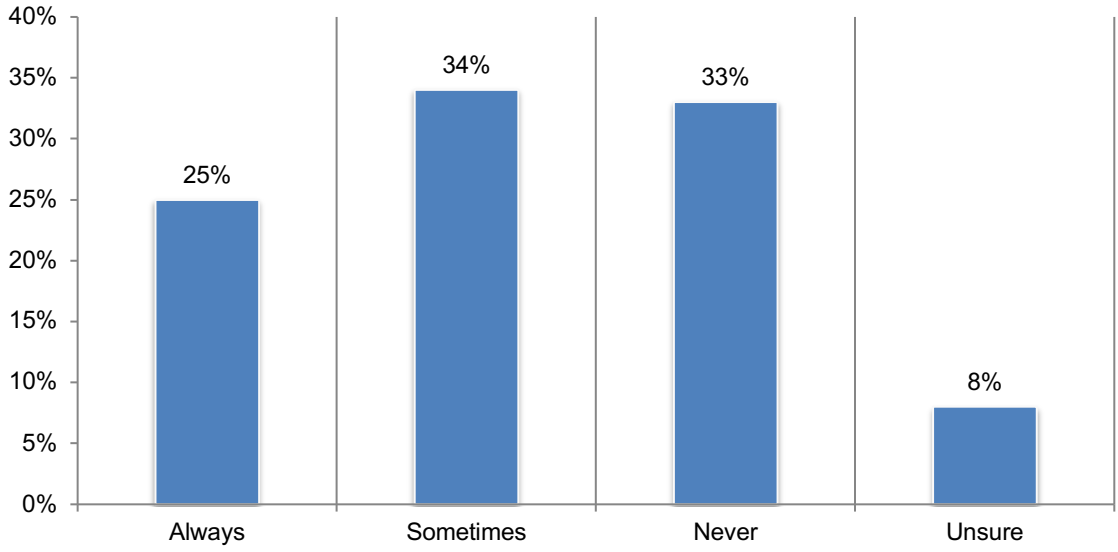
Figure 12. How does your organization categorize suppliers?
Only one choice permitted



There is a lack of integration between procurement and/or contracting departments and the SCRM process that could affect the ability of contracts to ensure the security of the supply chain. Only 41 percent of respondents say the procurement and/or contracting departments are integrated with their organization's SCRM process.

As shown in Figure 13, only 25 percent of respondents say their organizations always add supplier remediations into their contracts if needed.

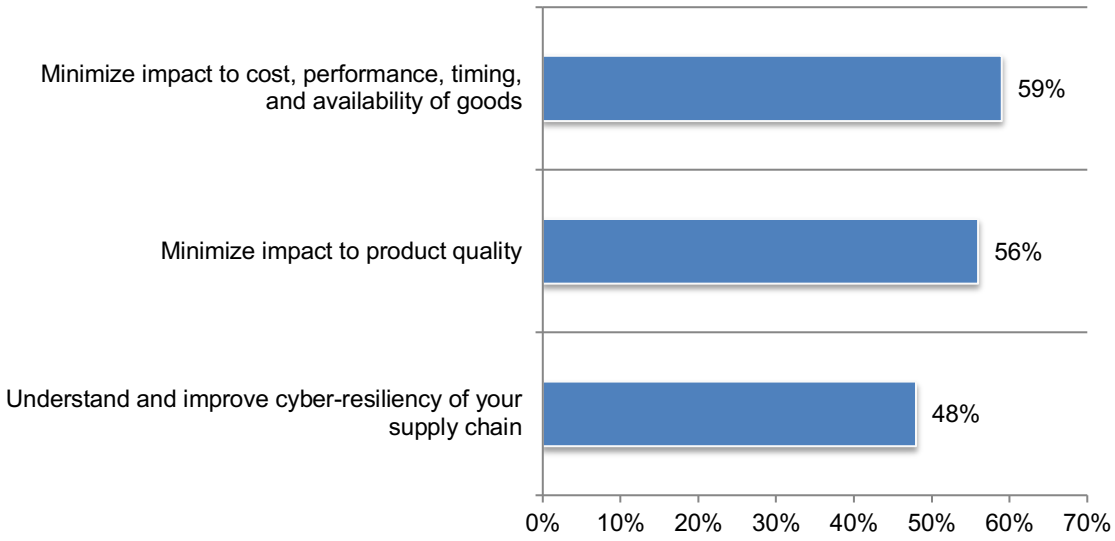
Figure 13. Do you add supplier remediations into your contracts if needed?



The current and future state of SCRM healthcare programs

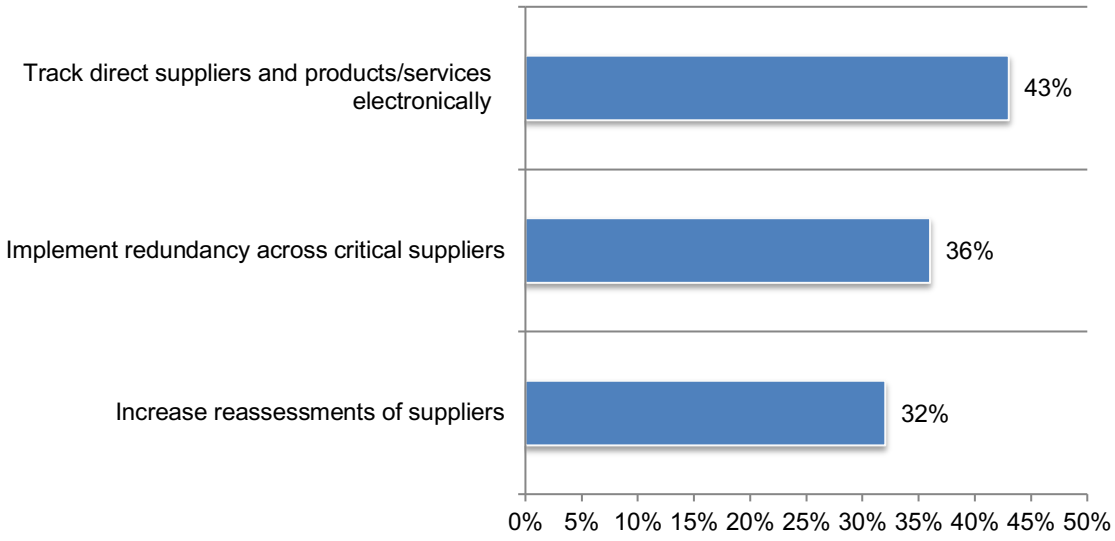
Business goals for SCRM are focused on cost, product quality and the supply chain. Respondents were asked to identify the business goals driving the SCRM program. According to Figure 14, 59 percent of respondents say their organizations are prioritizing the minimization of the impact to cost, performance, timing and availability of goods followed by 56 percent of respondents who say it is to minimize the impact of product quality. Almost half (48 percent of respondents) say it is to understand and improve cyber-resiliency of their supply chain.

Figure 14. What are your organization's top three business goals for SCRM?
Top three responses presented



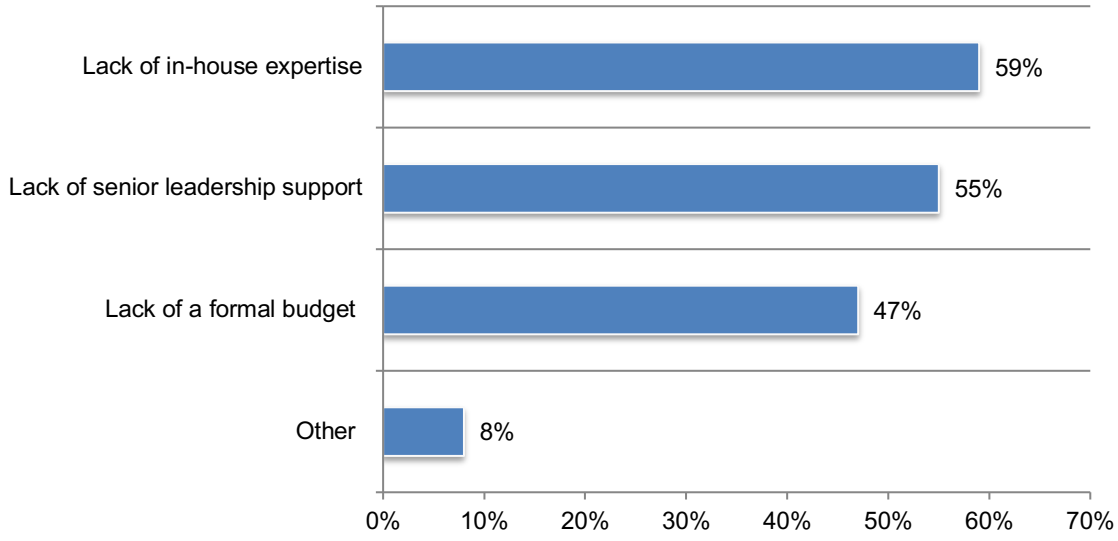
Organizations are focused on tracking direct suppliers and products/services electronically (43 percent of respondents). Other top priorities are to have redundancy across critical suppliers and increase reassessments of suppliers, 36 percent and 32 percent of respondents respectively.

Figure 15. What are the top three priorities of your organization's SCRM program?
Top three responses presented



Healthcare organizations face the challenge of having the in-house expertise and senior leadership needed to have a successful SCRM program. Respondents were asked to select the reasons for not having an effective SCRM program. As shown in Figure 16, 59 percent of respondents say it is the lack of in-house expertise and 55 percent of respondents say it is a lack of senior leadership support.

Figure 16. What are your organization's barriers to having a successful SCRM program?
More than one response permitted

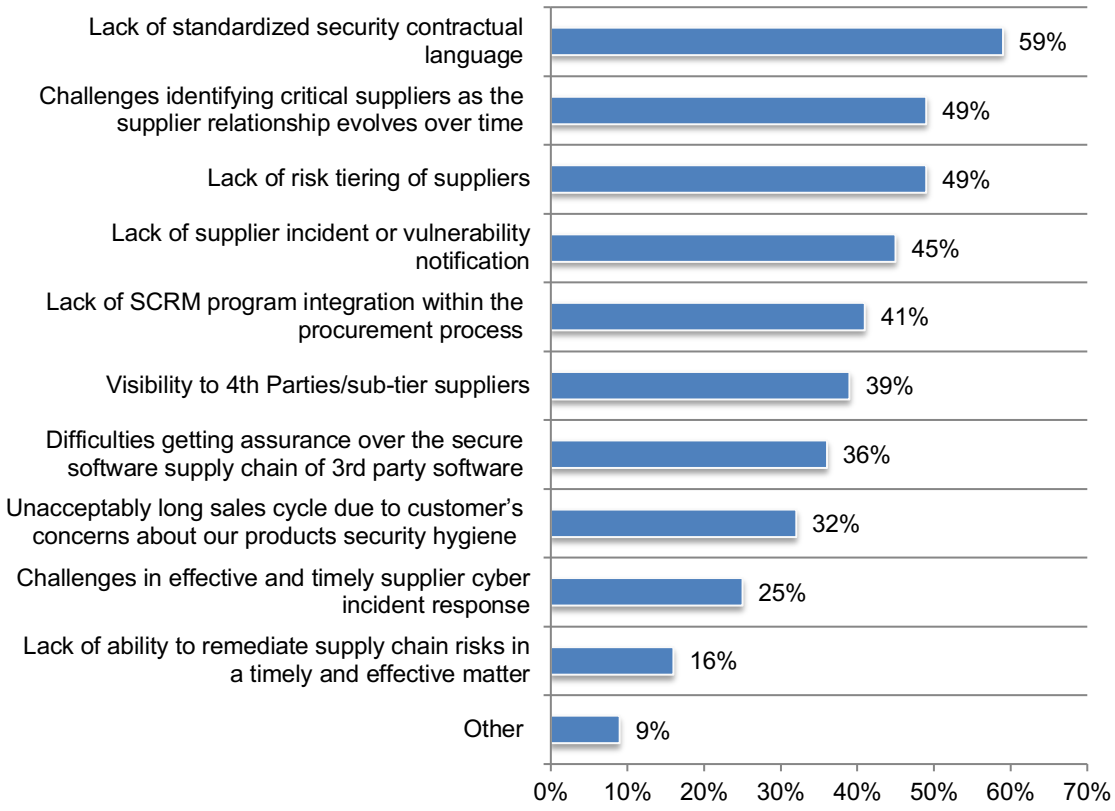


A lack of cooperation from suppliers and employees is the primary people-related impediment to a successful SCRM program. Figure 17 presents a list of barriers to an effective SCRM program due to the behaviors of suppliers and the various functions within healthcare organizations. As shown, 54 percent of respondents say the lack of co-operation from suppliers and 43 percent of respondents say it is the lack of inter-departmental co-operation that stands in the way of having an effective program. According to the research, improving the supply chain cyber-resiliency is a critical business goal.

Figure 17. What are the main people-related impediments or challenges to achieving an effective SCRM program?
More than one response permitted

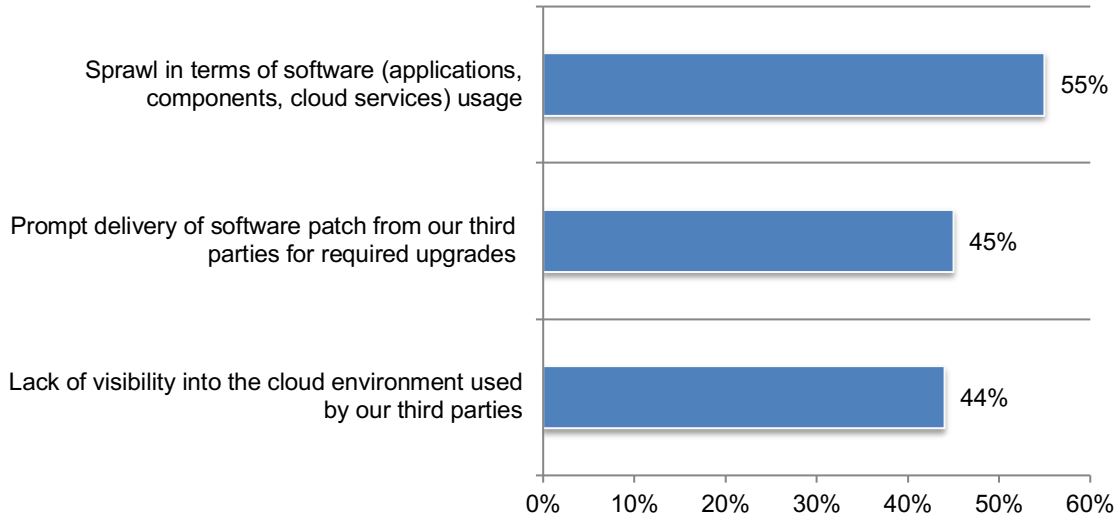
The lack of standardized language in security contracts and supply chain issues hinder an effective SCRM program. According to Figure 18, in addition to the lack of standardized security contractual language in contracts (59 percent of respondents), SCRM programs are affected by problems with the supply chain. These problems include challenges identifying critical suppliers as the supplier relationship evolves over time (49 percent of respondents), lack of risk tiering of suppliers (49 percent of respondents) and lack of supplier incident or vulnerability notification (45 percent of respondents)

Figure 18. What are the main process-related impediments or challenges to achieving an effective SCRM program?
Four responses permitted



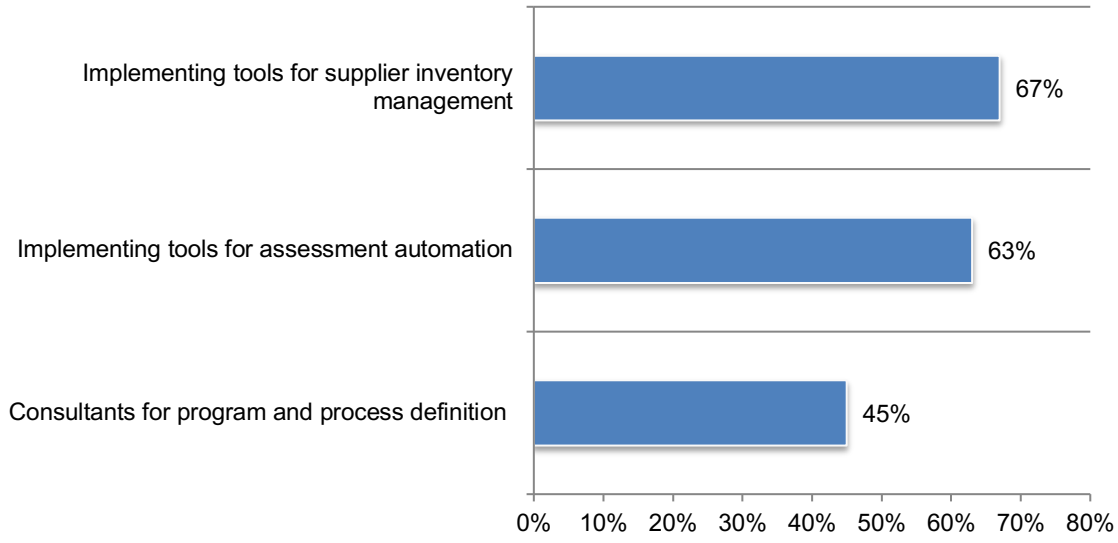
Controlling the sprawl of software usage is the number one technology-related impediment to achieving an effective SCRM program. As shown in Figure 19, a barrier to an effective SCRM program is managing the sprawl of software applications, components and cloud services, according to 55 percent of respondents. This is followed by the prompt delivery of software patches from third parties for required upgrades (45 percent of respondents) and the lack of visibility into the cloud environment used by third parties (44 percent of respondents).

Figure 19. What are the main technology-related impediments or challenges to achieving an effective SCRM program?
Top three responses presented



Improvement of supply chain management is a priority. According to Figure 20, 67 percent of respondents say their organizations' top priority is implementing tools for supplier inventory management. This is followed by 63 percent of respondents who say their organizations will be implementing tools for assessment automation and 45 percent of respondents say their organizations will hire consultants for program and process definition.

Figure 20. What are your organization's top three priorities for SCRM investments?
Top three responses presented



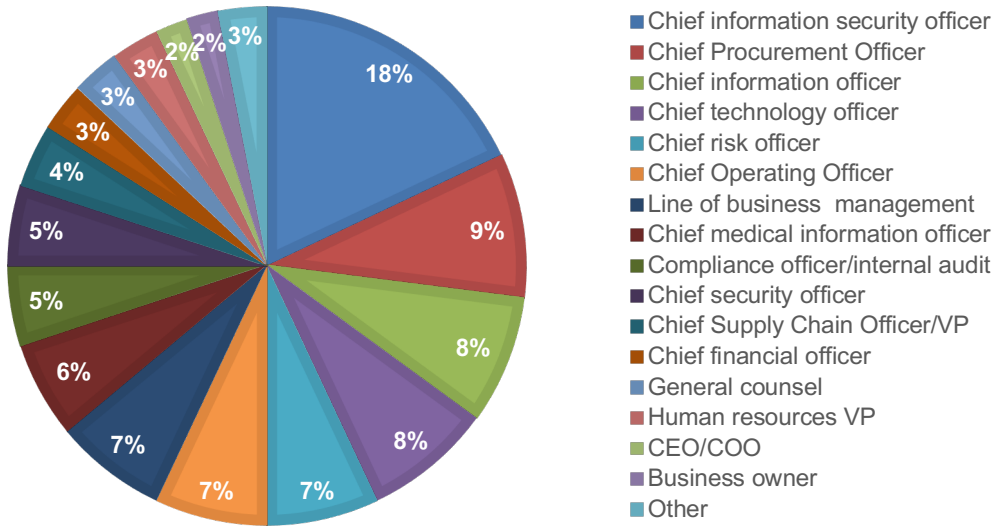
Part 3. Methodology

A sampling frame of 11,064 IT and IT security practitioners who are involved in their organizations' supply chain risk management program and are familiar with their cybersecurity plans or programs were selected as participants to this survey. Table 1 shows 463 total returns. Screening and reliability checks required the removal of 61 surveys. Our final sample consisted of 402 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	11,064	100.0%
Total returns	463	4.2%
Rejected or screened surveys	61	0.6%
Final sample	402	3.6%

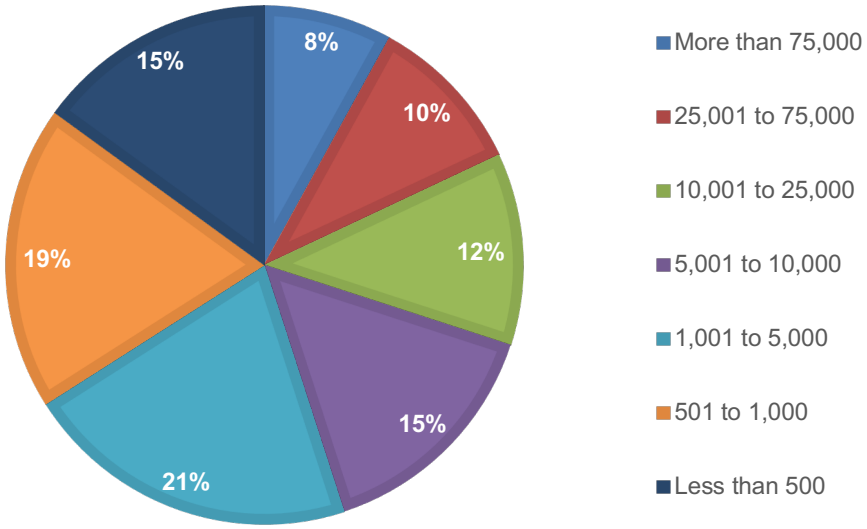
As shown in Pie Chart 1, 18 percent of respondents report to the chief information security officer, 9 percent of respondents report to the chief procurement officer, 8 percent of respondents report to the chief information officer, and 8 percent of respondents report to the chief technology officer.

Pie Chart 1. Direct reporting channel



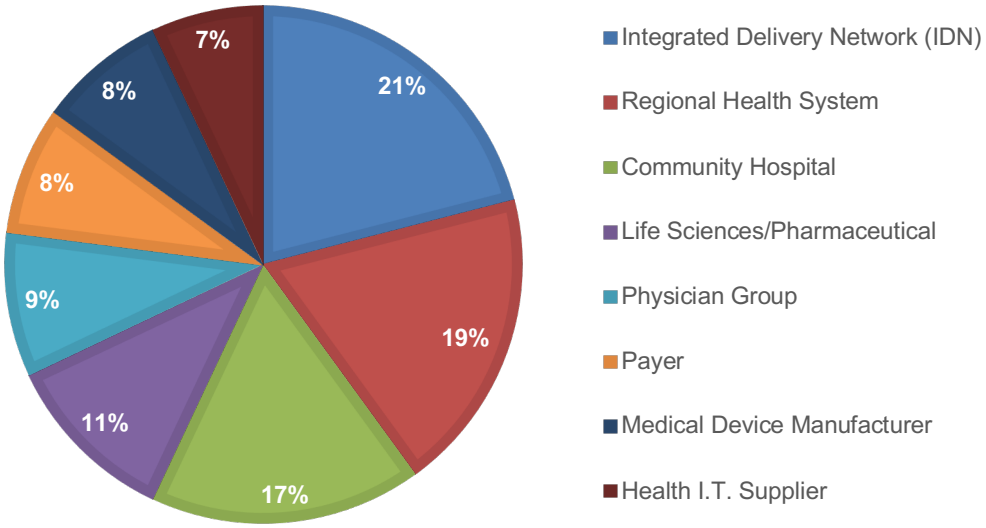
Almost half (45 percent) of respondents reported their organization employs more than 5,000 employees. The largest category at 21 percent of respondents is organizations that employ between 1,000 and 5,000 employees.

Pie Chart 2. The number of employees within the organization



Pie Chart 3 describes the respondents' organizations. Twenty-one percent of respondents say their organization is an integrated delivery network, this is followed by regional health system (19 percent of respondents), community hospital (17 percent of respondents), and life sciences/pharmaceuticals (11 percent of respondents).

Pie Chart 3. Type of organization



Part 4. Caveats to this study

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

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of 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 IT and IT security professionals. 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.

Part 5. Appendix with the detailed audited findings

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 2022.

Survey Response	Freq
Total sampling frame	11,064
Total survey returns	463
Rejected surveys	61
Final sample	402
Response Rate	3.6%

Part 1. Screening

S1. Are you part of a healthcare or life sciences organization?	Pct%
Yes	100%
No (Stop)	0%
Total	100%

S2a. Does your organization have a supply chain risk management program (SCRM)?	Pct%
Yes	100%
No (~~Stop~~)	0%
Total	100%

S2b. If yes, how familiar are you with the program?	Pct%
Very familiar	39%
Familiar	42%
Somewhat familiar	19%
Not familiar (Stop)	0%
Total	100%

S3a. Does your organization have a cybersecurity plan or program?	Pct%
Yes	100%
No (~~Stop~~)	0%
Total	100%

S3b. If yes, how familiar are you with the program?	Pct%
Very familiar	39%
Familiar	40%
Somewhat familiar	21%
Not familiar (~~Stop~~)	0%
Total	100%

Part 2. The management of supplier risk

Following are five (5) steps healthcare organizations normally take to manage supplier risks. Please rate how well your organization accomplishes each step using the four-pointed scale provided below each item: **fully and partially accomplished** responses combined..	Pct%
Q1a. Cybersecurity supply chain risk management processes are identified, established, assessed, manage accomplished, and agreed to by the organization's stakeholders.	58%
Q1b. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	53%
Q1c. Contracts with suppliers and third-party partners are used to implement measures to meet the objectives of our organization's cybersecurity supply chain risk management plan.	47%
Q1d. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	50%
Q1e. Response and recovery planning and testing are conducted with suppliers and third-party providers.	42%

Q2. Does your organization maintain an updated, digital & centralized inventory of suppliers of physical goods, business-critical services (including consulting services), and/or third-party information technology (including devices)?	Pct%
Yes, we have a complete inventory	19%
Yes, we have a partial inventory	38%
No	43%
Total	100%

Q3. Is your organization's SCRM program based on industry standards?	Pct%
Yes	49%
No	45%
Unsure	6%
Total	100%

Q4a. Do you leverage frameworks or industry guides in thinking about your SCRM posture? Please select all that apply .	Pct%
NIST	54%
CMMC	27%
HIC-SCRIM	23%
HITRUST	29%
ISO-27000	33%
Other (please specify)	5%
No, we do not leverage frameworks or industry guides (please skip to Q5)	33%
Total	204%

Q4b. If your organization leverages frameworks or industry guides, are they helpful to improving its SCRM program?	Pct%
Yes	51%
No	49%
Total	100%

Q5. Has your organization ranked your suppliers and third parties based on their importance?	Pct%
Yes	43%
No	51%
Unsure	6%
Total	100%

Q6. How does your organization identify its business-critical suppliers? Please select all that apply.	Pct%
Cost containment	56%
Volume	47%
Care delivery	63%
Sole source	21%
Revenue generation	30%
Availability	59%
Safety (i.e. patient, employee, environmental)	68%
Compliance	42%
Other (please specify	5%
Total	391%

Q7. Who has overall responsibility for your organization's SCRM strategy? Please check the one best choice.	Pct%
Chief Risk/Compliance Officer	14%
Chief Information Officer	17%
Chief Financial Officer	13%
Chief Information Security Officer	16%
Chief Privacy Officer	3%
Chief Supply Chain Officer	10%
No one person has overall responsibility	21%
Other (please specify)	6%
Total	100%

Q8a. Does your organization's SCRM program categorize suppliers?	Pct%
Yes	53%
No	47%
Total	100%

Q8b. If yes, how does your organization categorize suppliers? Please select one best choice.	Pct%
Nature of the products or services	43%
Data classification	40%
Connectivity or network access	10%
Other (please specify)	7%
Total	100%

Q9. What are your organization's top three business goals driving the SCRM program? Please select the top three choices only.	Pct%
Minimize impact to cost, performance, timing, and availability of goods	59%
Meet regulatory responsibilities	37%
Minimize potential impacts to customer satisfaction, brand reputation, and shareholder value	31%
Minimize impact to product quality	56%
Ensure integrity and continuity of accounting processes (e.g., account receivable and accounts payable)	23%
Protect Intellectual property and competitive advantage	40%
Understand and improve cyber-resiliency of your supply chain	48%
Other (please specify)	6%
Total	300%

Q10. Do you feel you have a good grasp on the strengths and weaknesses of your current SCRM program?	Pct%
Yes	63%
No	37%
Total	100%

Q11. What level of formal document does the SCRM program have? Please select one best choice.	Pct%
Policies only	34%
Policies and Standards	23%
Policies, Standards and Procedures	20%
No formal documentation	23%
Total	100%

Q12. Which of the following are included in the scope of your organization's SCRM program?	Pct%
New suppliers that have been onboarded since the establishment of the program	46%
Pre-existing suppliers that have been on-boarded before the establishment of the program	54%
Total	100%

Q13a. Are business-critical suppliers part of your organization's continuity/disaster recovery (BC/DR) plans?	Pct%
Yes	43%
No	50%
Unsure	7%
Total	100%

Q13b. If yes, does your organization conduct validation tests of its BC/DR program with your suppliers?	Pct%
Yes	38%
No	55%
Unsure	7%
Total	100%

Q14. Does your organization evaluate the risks impacting patient care outcomes created by the new supplier's organization?	Pct%
Yes	60%
No	35%
Unsure	5%
Total	100%

Q15. Does your organization evaluate the risks impacting patient care outcomes created by new suppliers' products?	Pct%
Yes	50%
No	40%
Unsure	10%
Total	100%

Q16. How often does your organization require a security evaluation of its business-critical suppliers? Please select one.	Pct%
On an ad-hoc basis	24%
Monthly	15%
Bi-monthly	13%
Annually	12%
Every two years	16%
Only when a security incident occurs	20%
Total	100%

Q17. What events trigger a security evaluation of business-critical suppliers? Please select all that apply.	Pct%
When contracts with suppliers are renewed	53%
When relationships with suppliers are changed	56%
When additional products are purchased from the suppliers	46%
None of these events would require a security evaluation	15%
Total	170%

Q18. What tools, technologies and services are used as part of your organization's supplier evaluation? Please select all that apply.	Pct%
Spreadsheets only	26%
GRC Platform	31%
Risk Ratings/Scoring Service	30%
Supply chain risk management platform	17%
Third-party risk platform	25%
Third-party risk management services	19%
Consultants	25%
Other tools and automation	30%
Total	203%

Q19. Does the SCRM program assess the integrity/provenance of suppliers' software and technology (e.g. Software Bill of Materials, Software Build Pipeline, Delivery Mechanisms)?	Pct%
Yes	43%
No	49%
Unsure	8%
Total	100%

Q20. Does your organization accept certifications (e.g. PCI-DSS, ISO-27001) in lieu of your usual assessment/attestation process for suppliers?	Pct%
Yes	43%
No	48%
Unsure	9%
Total	100%

Q21. Are procurement and/or contracting departments integrated with your organization's SCRM process?	Pct%
Yes	41%
No	47%
Unsure	12%
Total	100%

Q22. Do you add supplier remediations into your contract if needed?	Pct%
Always	25%
Sometimes	34%
Never	33%
Unsure	8%
Total	100%

Q23. Does your organization have on-going monitoring as part of your SCRM process? Please select all that apply.	Pct%
Yes, with continuous control assessments	49%
Yes, with automated monitoring/threat intelligence	45%
Yes, with supplier audit report, SOC2 or similar mechanism	31%
We do not have on-going monitoring	25%
Other (please specify)	6%
Total	156%

Q24. Does your organization's SCRM program extend to cover 4th-Party/Nth Tier suppliers?	Pct%
Yes	38%
No	62%
Total	100%

Q25. What are your organization's barriers to having a successful SCRM program? Please select all that apply.	Pct%
Lack of in-house expertise	59%
Lack of a formal budget	47%
Lack of senior leadership support	55%
Other (please specify)	8%
Total	169%

Q26. What is your organization's annual budget for its SCRM in 2022?	Pct%
Less than $250,000	10%
Between $250,000 and $500,000	21%
Between $500,000 and $1 million	23%
Between $1 and $2 million	26%
Between $2 and $5 million	11%
$5 million +	9%
Total	100%
Extrapolated value	$ 1,578,750

Q27. How will the budget increase or decrease?	Pct%
Increase by less than 5 percent	8%
Increase by 5 percent to 10 percent	9%
Increase by 10 percent to 15 percent	21%
Stay the same	35%
Decrease by less than 5 percent	12%
Decrease by 5 to 10 percent	8%
Decrease by more than 10 percent	7%
Unsure	0%
Total	100%
Extrapolated value	1.7%

Part 3. The future of SCRM programs in healthcare

Q28. What are your organization's top three priorities for SCRM investments? Please select the top three only.	Pct%
Implementing tools for assessment automation	63%
Implementing tools for supplier inventory management	67%
Consultants for program and process definition	45%
Implementing tools for tracking remediations	31%
Implementing tools for third-party risk scoring	17%
Additional staff	20%
Third-party auditors for reassessments	*31%*
Training staff on supply chain risk management processes and procedures	20%
Other (please specify)	6%
Total	300%

Q29. Does your organization plan to implement and use the following tools, technologies and services? Please select all that apply.	Pct%
Spreadsheets only	22%
GRC platform	33%
Ingest and utilize SBOMs	35%
Risk ratings/scoring service	34%
SCRM platform	36%
TPRM platform	21%
Outsourced services / managed service provider	15%
Other tools /services (please specify)	6%
Total	202%

Q30. What are the top three priorities of your organization's SCRM program? Please select three.	Pct%
Track direct suppliers and products/services electronically	43%
Implement electronic inventory of suppliers, product, services	29%
Track 4th party suppliers and products/services electronically	29%
Establish visibility into 4th-Party/Nth Tier suppliers	17%
Extend program to cover more of the current supplier base	23%
Increase reassessments of suppliers	32%
Implement redundancy across critical suppliers	36%
Incorporate software bill of materials in software supply chain assessments	27%
Outsource our supply chain risk management process to an external partner	25%
Implement a technology solution that automates our supply chain risk management process	18%
Training and education for team	16%
Other (please specify)	5%
Total	300%

Q31. What are the main people-related impediments or challenges to achieving an effective SCRM program? Please select all that apply.	Pct%
Lack of leadership support/executive sponsorship within the organization	25%
Lack of resources to develop or operate program enhancements	28%
Lack of appropriate SME skills to enhance or operate the program	33%
Lack of co-operation from suppliers	54%
Lack of inter-departmental co-operation	43%
Inability to hire qualified candidates to fill approved and funded vacancies	27%
Lack of knowledgeable/available point of contact on supplier side	25%
Other (please specify)	4%
Total	239%

Q32. What are the main process-related impediments or challenges to achieving an effective SCRM program? Please select the top four.	Pct%
Lack of risk tiering of suppliers	49%
Lack of SCRM program integration within the procurement process	41%
Lack of standardized security contractual language	59%
Lack of supplier incident or vulnerability notification	45%
Challenges identifying critical suppliers as the supplier relationship evolves over time	49%
Challenges in effective and timely supplier cyber incident response	25%
Visibility to 4th Parties/sub-tier suppliers	39%
Difficulties getting assurance over the secure software supply chain of 3rd party software	36%
Unacceptably long sales cycle due to customer's concerns about our products security hygiene	32%
Lack of ability to remediate supply chain risks in a timely and effective matter	16%
Other (please specify)	9%
Total	400%

Q33. What are the main technology-related impediments or challenges to achieving an effective SCRM program? Please select the top three	Pct%
Lack of visibility into the cloud environment used by our third parties	44%
Lack of clarity on how our third parties access the data we share with them	39%
Lack of clarity on data storage locations and practices of our third parties	31%
Prompt delivery of software patch from our third parties for required upgrades	45%
Sprawl in terms of software (applications, components, cloud services) usage	55%
Cost of technology	27%
Lack of integration of technology with existing supply chain applications/workflows	21%
Immature supplier product security	19%
Product security incident response	16%
Other (please specify)	3%
Total	300%

Part 4. Organizational characteristics

D1. Check the Primary Person you report to within the organization	Pct%
CEO/COO	2%
Business owner	2%
Chief financial officer (CFO)	3%
General counsel	3%
Chief information officer (CIO)	8%
Chief technology officer (CTO)	8%
Chief risk officer (CRO)	7%
Chief information security officer (CISO)	18%
Chief medical information officer (CMIO)	6%
Compliance officer/internal audit	5%
Chief Supply Chain Officer/VP	4%
Chief Procurement Officer (CPO)	9%
Chief Operating Officer (COO)	7%
Human resources VP	3%
Chief security officer (CSO)	5%
Line of business (LOB) management	7%
Other (please specify)	3%
Total	100%

D2. How many employees are in your organization?	Pct%
Less than 500	15%
501 to 1,000	19%
1,000 to 5,000	21%
5,001 to 10,000	15%
10,001 to 25,000	12%
25,001 to 75,000	10%
More than 75,000	8%
Total	100%

D3. Which of the following best describes your organization?	Pct%
Integrated Delivery Network (IDN)	21%
Regional Health System	19%
Community Hospital	17%
Physician Group	9%
Payer	8%
Life Sciences/Pharmaceutical	11%
Medical Device Manufacturer	8%
Health I.T. Supplier	7%
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.