DARK Reading

REPORTS

Next

August 2023

The State of Supply Chain Threats

Widely exploited vulnerabilities in open source software and malicious components being loaded in trusted public repositories have highlighted issues in the software supply chain. Here’s what organizations are doing to mitigate their risk.

Sponsored by mend.io

informa tech

TABLE OF CONTENTS

Figures

Sponsored Content

MEND PERSPECTIVES

By Carol Hildebrand

The Rising Threat of Malicious Packages

Malware has entered the software supply chain. Are you prepared?

Open source code package repositories, such as npm and RubyGems, allow anyone to store or publish packages, and unfortunately, even those containing malware. These are known as malicious packages — the malware of the software supply chain.

Malicious packages aren't new, but they're proliferating at an alarming pace. In our "Special Report: Software Supply Chain Malware," Mend.io identified a 315% increase in malicious packages published to npm and RubyGems from 2021 to 2022, and expects that trend to continue.

Anatomy of a Malicious Package Attack

Malicious packages are used to steal credentials, exfiltrate data, turn applications into botnets, or erase data. But first, attackers need to trick someone or something into downloading the package.

It can be as simple as hiding a malware payload in open source code and tricking a careless developer into using it, or elevating bugs in package manager systems and then benefiting from the opportunities afforded by the scale of a corrupted software supply chain. Make no mistake: Like any malware, malicious packages can inflict significant damage.

Organizational Impact: Malicious Packages Are More Dangerous Than Vulnerabilities

Once a developer downloads a malicious package, how much damage it does will depend on the following factors:

1. Intent: When threat actors infiltrate using a malicious package, their intent substantially determines the impact. A threat actor trying to inform people about a war or protest action with annoying messages has a lower overall impact than one trying to steal information or turn developers' machines into cryptocurrency miners.

2. Organization type: Attacks designed to exfiltrate personal information will have a larger, potentially long-term impact on companies trusted with sensitive data. Ransomware attacks that disable systems can have an outsize impact in organizations like hospitals, where lives depend on uptime.

3. Duration: When malicious packages are discovered quickly and removed completely, the damage they cause can be limited. The greatest damage can be caused by packages that remain undetected for months or years while quietly delivering their payloads.

4. Spread: Some of the most dangerous malicious packages are designed to provide initial access to a network, at which point the threat actor can move laterally through systems to steal passwords or protected information to gain even more access.

Unlike vulnerabilities, which can and do often exist for months or years in application code without being exploited, a malicious package represents an immediate threat to your organization.

Malicious Package Attack Vectors

To deliver a malicious payload via an open source package, attackers must find a way to get the package downloaded. The four

Previous Next

Table of Contents

basic attack vectors for malicious packages are brandjacking, typosquatting, dependency hijacking, and dependency confusion.

Brandjacking: An attacker acquires or otherwise assumes the online identity of another company or an owner of a package and then inserts a malicious code. It doesn't necessarily mean he actively steals something, but just takes advantage of an opportunity to take ownership related to the brand name.

Typosquatting: An attacker publishes a malicious package with a similar name to a popular package, in the hope that a developer will misspell a package name and unintentionally fetch the malicious version.

Dependency hijacking: An attacker obtains control of a public repository in order to upload a new, malicious version.

Dependency confusion attacks: Here, the threat actor creates a public repository package with the identical name of an internal package within the intended target system. The intention is to trick the target's dependency management tools into downloading the malicious public package instead of the safe internal one.

The best defense against the growing threat of malicious packages is a knowledgeable and alert developer community in and around open source registries, combined with automated detection and response solutions.

Read Mend.io's "Special Report: Software Supply Chain Malware" for the latest research on the malware of the supply chain.

About the Author: *A veteran of Computerworld and CIO magazine, Carol Hildebrand is an award-winning technology writer who focuses on cybersecurity and how it impacts business innovation.*

About the Author

Fahmida Y. Rashid
Dark Reading

Fahmida Y. Rashid is Dark Reading's managing editor for features. She has spent over a decade analyzing news events and demystifying security technology for IT professionals and business managers. Her work has appeared in various business and tech trade publications, including VentureBeat, CSO Online, InfoWorld, eWEEK, and CRN.

EXECUTIVE SUMMARY

Many organizations changed — or started making significant changes to — their supply chain security practices two years ago to address growing risks from vulnerable third-party software and open source components. On the open source front, the growing number of malicious components being pushed into public code registries — such as npm, PyPI, and Maven — highlights the necessity of these changes. More concerning for organizations is the fact that attackers have exploited zero-day vulnerabilities in multiple, widely used software products, including Microsoft Exchange, Kaseya, and Accellion, to breach numerous government and private entities worldwide.

Dark Reading's 2023 Supply Chain Threat Survey of 242 IT and cybersecurity professionals shows that a lot has stayed the same in regard to supply chain risk. A relatively high percentage of organizations have implemented processes for mitigating risk from vulnerabilities in the partner ecosystem, and there is strong awareness of what needs to be done to strengthen the security of the software supply chain. Most organizations, for instance, maintain a software bill of materials repository, and more than one-third of respondents expect their organizations to increase their use of SBOMs in the coming year.

More than half the organizations in Dark Reading's survey require their software suppliers to adhere to stipulated security standards, and nearly one in four want their vendors to submit independent audits or assessments indicating they meet security requirements. Others request ad hoc, point-in-time assessments of their suppliers' security posture.

What is striking about this report is that different occurrences have affected responses this year versus last. The attacks against Kaseya and Accellion were fresh in the minds of the respondents last year; this year's respondents were asked to assess their ability to detect and mitigate supply chain attacks while being confronted with the attacks that exploited multiple vulnerabilities in the MOVEit file transfer utility.

While many organizations have implemented multiple processes for managing supply chain risks, a sizable percentage of organizations have not done so and remain at heightened exposure to attacks via the supply chain. Even so, most IT and cybersecurity professionals in the survey appear confident in their organizations' ability to defend against a supply chain attack and to detect and respond to any incidents that might get past their defenses.

The following are some of the key takeaways from the survey:

- 71% of respondents describe third-party risk and supply chain security as one of their top five security initiatives for the coming year.

- 71% of organizations in the survey say their current security programs cover software supply chain threats, but only 28% explicitly state that their program covers the software supply chain.

- Just 24% of organizations consider their software supply chain secure. For 55% of organizations, software supply chain security is still a work in progress.

- 50% maintain a software bill of materials repository, but just 36% claim to create complete SBOMs for all their software. Just 41% regularly request SBOMs from vendors and suppliers.

- 40% say vulnerabilities in open source software components is their biggest supply chain-related worry; 24% point to developers being tricked into malicious components, via methods such as typosquatting and dependency confusion.

- 34% of respondents who had experienced a supply chain attack over the past year say developers accidentally downloaded malicious components from public code registries, such as PyPI and npm.

- 49% of IT and cybersecurity professionals in the survey say they are most concerned about attackers targeting their organizations via vulnerabilities in widely used commercial platforms.

Previous
Next
Table of Contents

SYNOPSIS

RESEARCH

Survey Name: Dark Reading 2023 Supply Chain Threat Survey

Survey Date: June 2023

Number of Respondents: 242 IT and cybersecurity professionals at companies of all sizes, based primarily in North America. The margin of error for the total respondent base (N=242) is +/-6.3 percentage points.

Purpose: Dark Reading surveyed information technology and cybersecurity professionals on the supply chain threat landscape; their biggest current concerns; the practices they have implemented to manage supply chain risk; and their capabilities for preventing, detecting, and responding to supply chain-related security issues.

Methodology: The survey queried decision-makers with job titles that involved IT or IT security (cybersecurity) at organizations across more than a dozen industry sectors. It asked them about a wide range of supply chain threats and risk mitigation practices. The survey was conducted online. Respondents were recruited via an email invitation containing an embedded link to the survey. The email invitation was sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

Dark Reading Reports

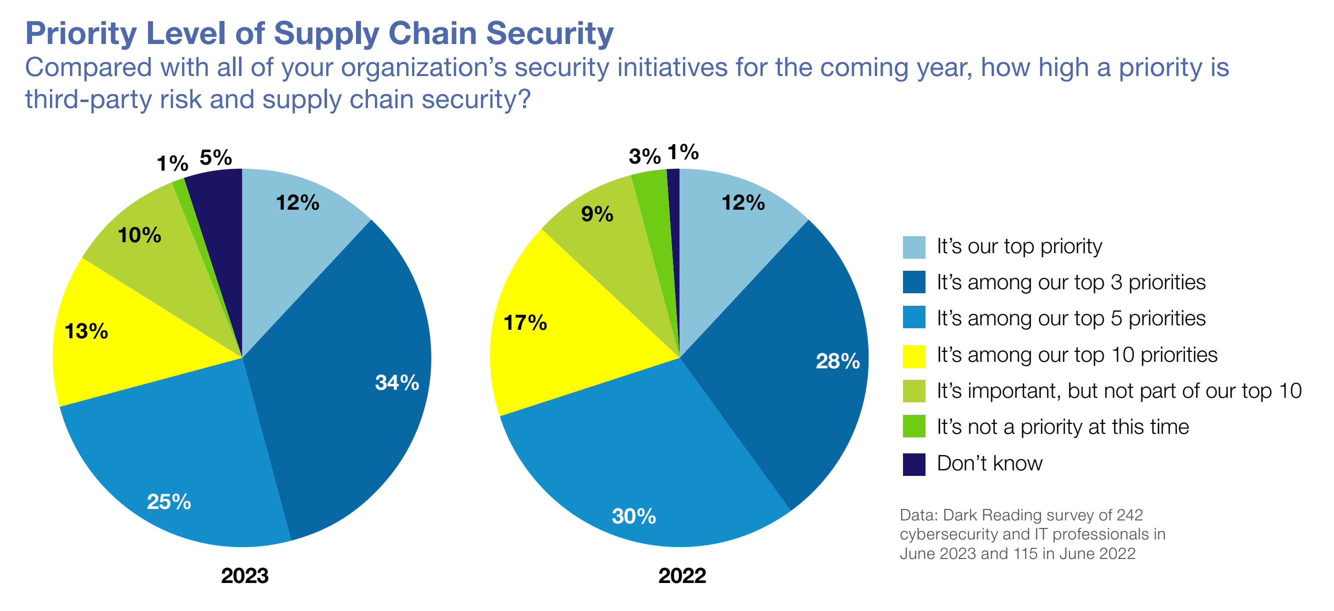
Previous Next
Table of Contents

High Concerns Over Supply Chain Risk

Supply chain security was in the headlines for most of 2022 — as well as the first half of 2023 — and it became increasingly clear that "supply chain risk" does not mean the same thing to everyone. Supply chain is one item under application security as organizations worry about the security and provenance of software components used in application development. Supply chain is also an item under security operations and cloud security as organizations scrutinize the security preparedness of their cloud providers and third-party service providers. Supply chain is also top of mind for organizations that are seeing their data stolen and networks compromised because a business application they rely on has been compromised.

These varied incidents highlight the damage supply chain attacks could cause and heightened concerns about enterprise exposure to different types of supply chain risks. But there are also signs to be optimistic about, such as industrywide efforts to strengthen the security of the software supply chain. Last year's executive order from the Biden administration requiring federal agencies to adopt a number of software security best practices — such as maintaining a software bill of materials for all software in use, implementing controls to protect build environments, and documenting all software dependencies in use — has pushed organizations to include those conversations as they make their security plans.

Figure 1.



Priority Level of Supply Chain Security

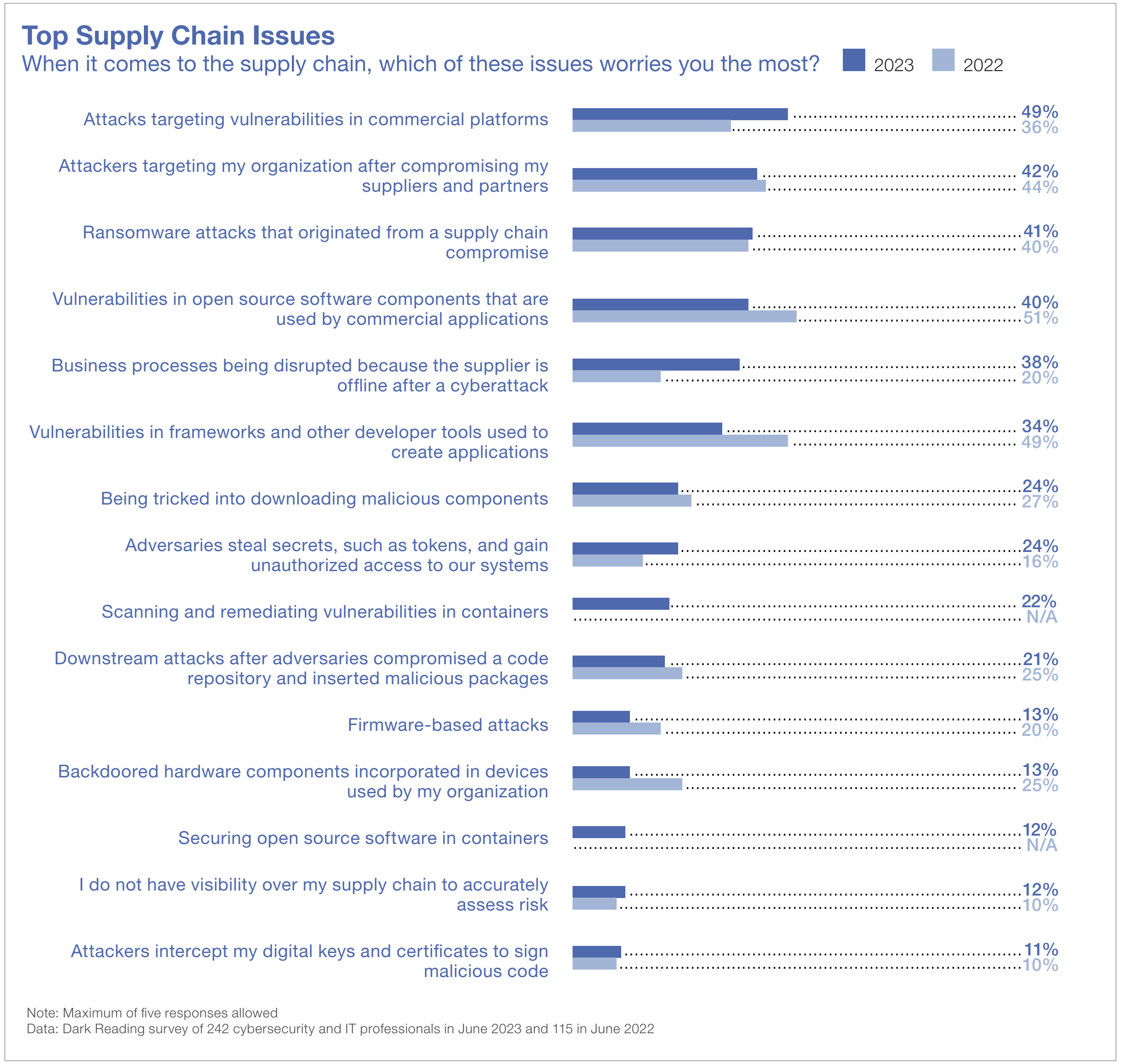
Compared with all of your organization's security initiatives for the coming year, how high a priority is third-party risk and supply chain security?

Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Dark Reading's 2023 Supply Chain Security Survey reflects this heightened sense of awareness. Supply chain security remains a major concern for IT and security professionals, with 71% of all organizations listing supply chain security among their top five security priorities for 2023. It tops the list of security priorities for 12% of organizations. What's noteworthy is that priorities don't seem to have shifted at all since last year, when 70% listed supply chain security among their top five **(Figure 1)**.

There is no clear consensus among security and IT decision-makers on which supply chain security issue concerns them most. Almost half (49%) of respondents cite attacks targeting vulnerabilities in commercial platforms as their biggest supply chain security issue, which is a significant increase from last year (36%) **(Figure 2)**. Some of the jump could be directly related to the fact that the survey was conducted around the time when researchers warned that

Figure 2.



Top Supply Chain Issues

When it comes to the supply chain, which of these issues worries you the most?

Note: Maximum of five responses allowed
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

attack groups were actively exploiting a critical zero-day vulnerability in Progress Software's MOVEit Transfer managed file transfer utility to steal data from organizations. Recent analysis from Brett Callow, a threat analyst at Emsisoft, suggests that 347 organizations have been affected and more than 18.6 million individuals had their data compromised.

Perhaps influenced by the attacks targeting MOVEit, respondents to the Dark Reading survey also list concerns that attackers would target their organizations after compromising suppliers and partners (42%), ransomware attacks originating from a supply chain compromise (41%), and disruptions to business processes because the supplier was hit by a cyberattack (38%).

Respondents are also concerned about their exposure to insecure open source components, tools, and frameworks. Forty percent of the respondents say their biggest supply chain security issue has to do with vulnerabilities in open source software components, and 34% say the same about flaws in frameworks and other tools developers use to create applications. About a quarter of respondents (24%) are concerned about their developers being tricked into downloading malicious components.

Typosquatting names and dependency poisoning are types of attacks in which a threat actor introduces malicious components into widely used public software repositories, such as npm, and then tries to trick users into downloading it by, for instance, using the local phone number from a legitimate package.

Enterprise supply chain security also goes beyond software: 13% cite firmware-based attacks as a major concern, and an equal number worry about backdoored hardware components used in devices.

From a risk prioritization standpoint, IT and security leaders are less focused on attacks targeting the partner ecosystem and more focused on mitigating exposure from vulnerable software. The respondents identify software as the most important issue when asked to rank supply chain risks by order of importance. Survey respondents rank risks associated with third-party vendors and contractors third, and other risks associated with open source software fourth, in order of importance **(Figure 3)**.

Third-party libraries are widely used in software development because they give developers a way to quickly add specific functionality to their code. But because the components can nest several layers in the code, sometimes it can be hard to find vulnerabilities in applications.

Work in Progress: Software Supply Chain Security

Dark Reading's survey shows most respondents are confident about the controls they have in place to mitigate supply chain security risks. Survey respondents express some level of confidence in how their organization would respond to a supply chain attack. Seventy percent indicate their organizations have designated staff to respond to supply chain issues or know whom to call in case of a supply chain attack, and 67% say their organizations have clear processes on how to respond **(Figure 4)**. Respondents also suggest they have all the pieces in place to be able to address and mitigate supply chain issues within one to three days (35%). There are roughly equal numbers of respondents with the confidence in their processes to be able to handle an incident in less than 24 hours (22%) and those requiring four days to approximately a week (19%) **(Figure 5)**. This suggests some variability remains in the kind of controls in place.

Figure 3.

Importance of Supply Chain Risks

Rank the following types of third-party and supplier risk to your organization in order of importance.

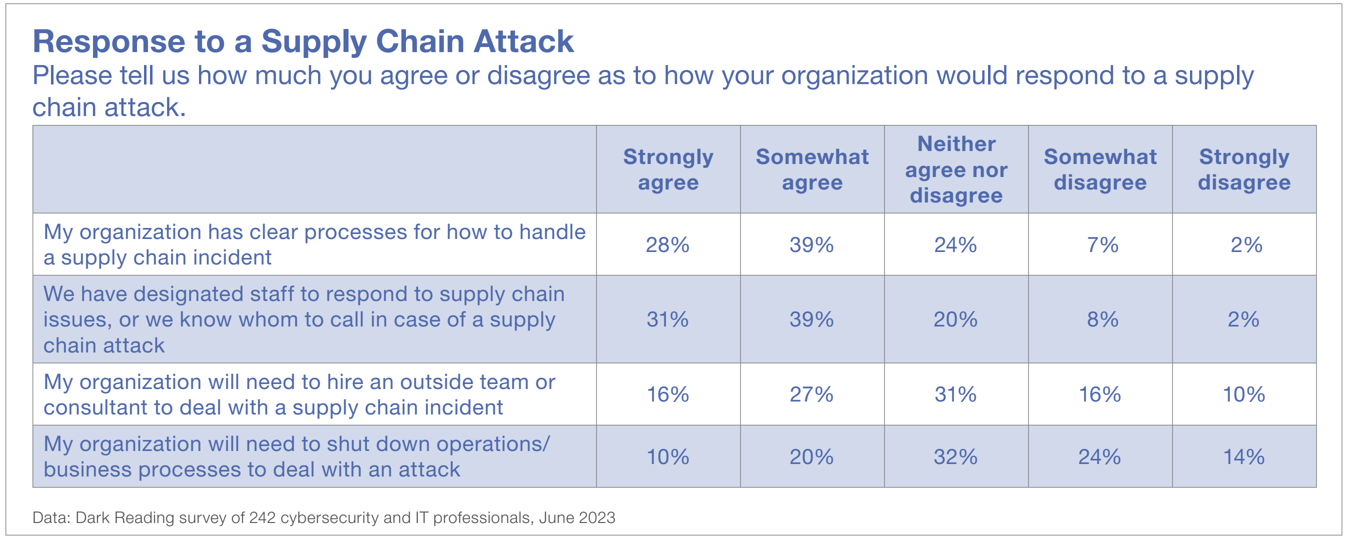
	Overall Rank	Score
Software	1	1,101
Digital supply chain	2	1,020
Third-party vendors and contractors	3	993
Open source software	4	943
Firmware	5	665
Container security	6	596
Hardware components	7	580

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.
Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

The confidence these results reflect did not carry over into the respondents' perception of the overall state of their organizations' software

Previous Next
Table of Contents

Figure 4.



Response to a Supply Chain Attack

Please tell us how much you agree or disagree as to how your organization would respond to a supply chain attack.

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
My organization has clear processes for how to handle a supply chain incident	28%	39%	24%	7%	2%
We have designated staff to respond to supply chain issues, or we know whom to call in case of a supply chain attack	31%	39%	20%	8%	2%
My organization will need to hire an outside team or consultant to deal with a supply chain incident	16%	27%	31%	16%	10%
My organization will need to shut down operations/ business processes to deal with an attack	10%	20%	32%	24%	14%

Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

supply chain security. Less than a quarter (24%) perceive their software supply chain to be fully secure, and almost an equal number (23%) say they have "a ways to go" to secure the software supply chain **(Figure 6)**. A third (33%) describe their efforts as a work in progress, either almost or halfway finished.

When asked to rank issues in software supply chain security, respondents say they are worried about vulnerabilities in third-party libraries, followed by developers downloading and importing malicious packages and components, and attackers tampering with existing libraries and repositories to include malicious code **(Figure 7)**. What's troubling is that despite these concerns, many organizations have not implemented controls to protect their software supply chain and to limit damage. Forty percent restrict their developers in using dependencies only from trusted repositories and registries, and just 36% regularly check container images for vulnerabilities as part of their processes for managing supply chain risk **(Figure 8)**. Security analysts consider such scanning — before a container is deployed into production — a fundamental practice for early risk detection and remediation.

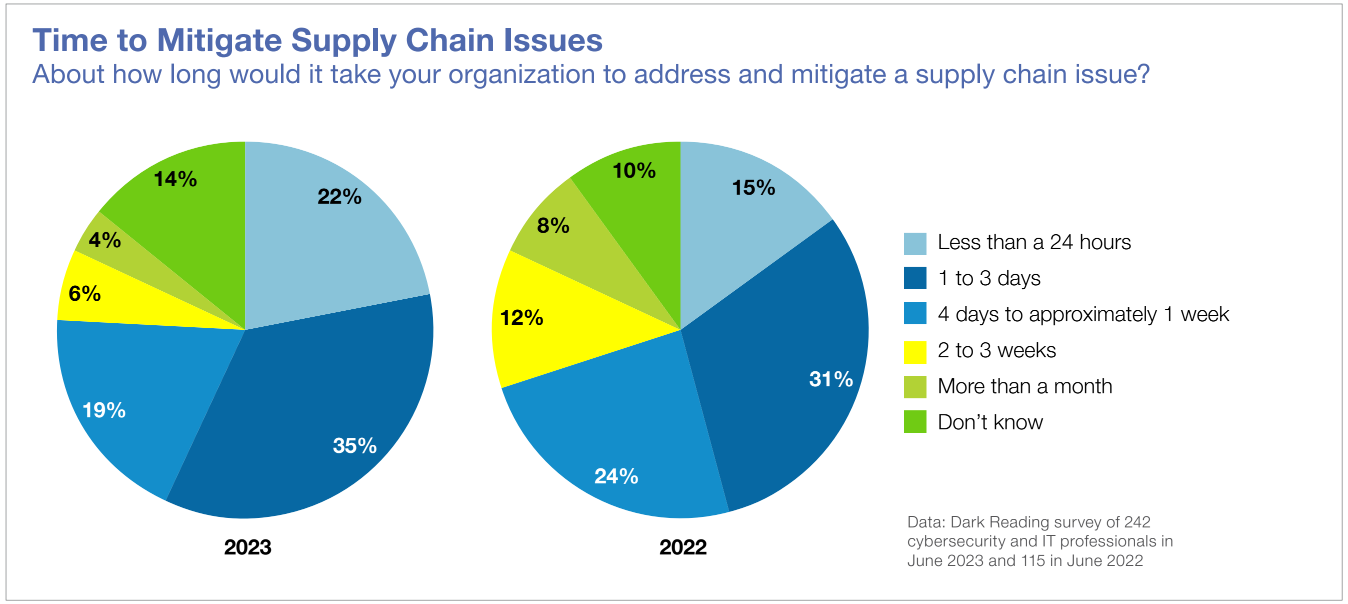
The use of vendor scorecards or rating scores from industry consortiums to assess the security of open source components remains an open question. While a plurality, 47%, say they do use some kind of scorecard system to assess software components, the fact that 20% are unsure if their organizations rely on vendor scorecards or rating scores to determine the security of open source components suggests the idea is still in the early stages **(Figure 9)**.

On the other hand, Dark Reading's 2023 Supply Chain Threats Survey reveals relatively high awareness and adoption of one supply chain best practice: the software bill of materials. Half (50%) of organizations maintain a software bill of materials repository, and 48% plan on increasing SBOM use over the next year **(Figure 10)**. An SBOM, an inventory of all open source and third-party components used in a particular piece of software, typically includes information such as the license of the software component, its version, and list of known vulnerabilities that may be present. Security experts see SBOMs as key to an organization's ability to quickly identify and remediate vulnerabilities in open source components in their software. However, the use of SBOMs still seems limited, as only 41% regularly request SBOMs from their vendors and suppliers, and the same percentage of respondents uses SBOMs as part of their vulnerability management efforts.

Just a third (33%) have deployed automated tools to minimize human input and reduce the attack surface, and another third (32%) accept only signed components and verify signatures before deployment. Other processes for managing the software supply chain include verifying the changelog and commit history for a particular code component or software project before downloading it (26%), and signature verification before deployment and executing application builds in ephemeral, sealed, or isolated environments (25%).

Respondents were also asked to share their perceptions of how difficult it is to implement build practices and methods for preventing, mitigating, and remediating software supply chain security attacks. The results suggest there is some work left to do. While the respondents tend to be neutral (rating three on a five-point scale), a significant number consider the practices difficult. Forty-three percent say using a hermetic build with all inputs declared with immutable references is difficult **(Figure 11)**. Making provenance information — when, where, and how the software was produced — available is one way to ensure the application hasn't been tampered with, but 32% report that this action is difficult to implement. While respondents agree that shifting left is necessary to secure the software supply chain (55%), the mechanism for doing so remains a daunting process for many of them **(Figure 12)**.

Figure 5.



Time to Mitigate Supply Chain Issues

About how long would it take your organization to address and mitigate a supply chain issue?

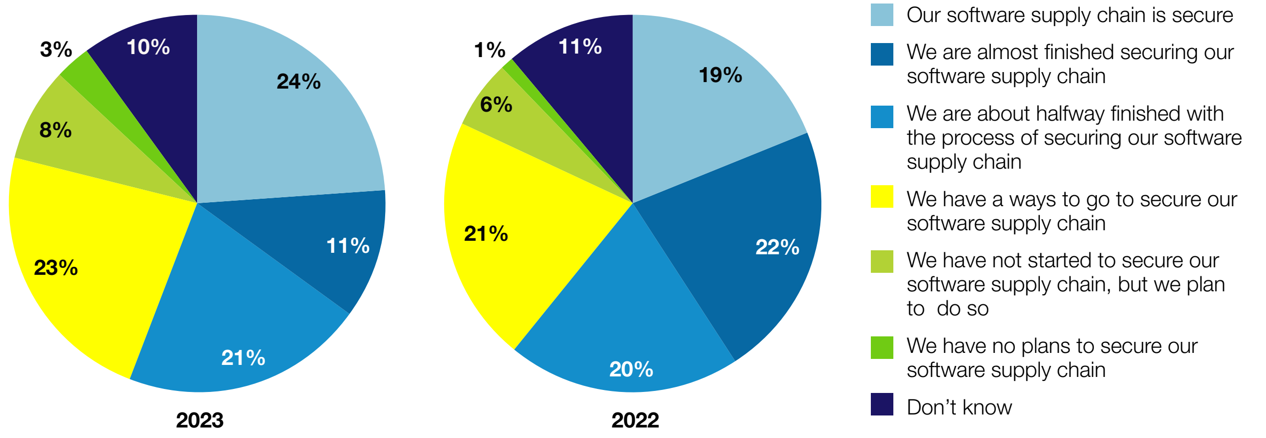
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Profound Impact on Supply Chain Practices

Breaches resulting from recent vulnerabilities in widely used third-party software and open source components are having a profound effect on enterprise supply chain security practices. The incidents have pushed many organizations over the past year to change — or start making changes to — their approach to managing supply chain risks. Fifty-six percent of organizations surveyed have made some kind of changes to address risks from third-party suppliers and partners; 17% are in the process of making major changes **(Figure 13)**. Last year, 65% made changes of some sort (including major ones). What's more, supply chain concerns in the wake of the attacks against MOVEit would likely push organizations to revamp their practices again on how they handle third-party software and open source risk.

More than half (51%) of responding organizations have stipulated security practices that vendors must adhere to as part of their

Figure 6.



State of Software Supply Chain

What is the state of your organization's software supply chain security?

Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

contract, and 39% require vendor security self-assessments **(Figure 14)**. When organizations ask vendors to conduct self-assessments, they are looking for information such as vulnerability management information (68%), data security controls being used (60%), documentation on the vendor's design and testing process (44%), and the vendor's asset inventory and user management practices (41%) **(Figure 15)**. About a third of respondents (35%) want answers to questions pertaining to the vendor's supply chain levels for software artifacts (SLSA), and 38% want a list of vulnerable packages.

The use of vendor security risk assessment questionnaires has become more widespread, and numerous standardized questionnaires are readily available for organizations to adapt for their use. Among the most widely used are the Shared Assessment Group's Standardized Information Gathering (SIG) questionnaire, the National Institute of Standards and Technology (NIST) vendor questionnaire, and the Vendor Security Alliance questionnaire.

Nearly three-quarters, or 74%, of organizations require multifactor authentication for third-party access to secure environments, and 57% enforce least-privilege access rules **(Figure 16)**. Nearly half (49%) of organizations have segmented their networks to limit lateral movement; 34% require vulnerability scanning of vendor systems; and 22% rely on code analysis, including binary analysis.

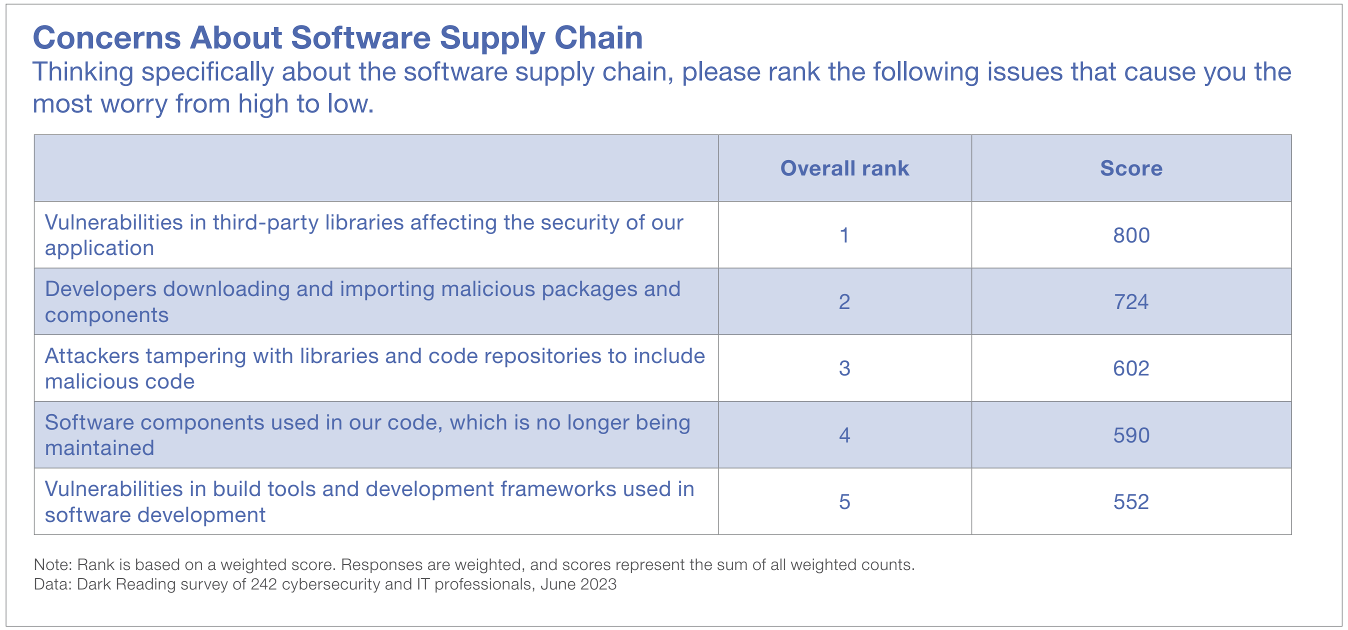
The survey shows that concerns about supply chain attacks may be theoretical for many enterprises. Just a quarter (24%) of respondents say they have experienced supply chain attacks over the past year, but 60% state they have not **(Figure 17)**. Among the victims, the two most common types of attacks were those targeting the partner ecosystem (43%) and those exploiting vulnerabilities in software components (41%) **(Figure 18)**. Despite concerns about typosquatting and dependency confusion, only about a third (34%) of respondents who had experienced a supply chain attack say their developers had accidentally downloaded malicious components from public repositories, such as npm, PyPI, and Maven.

Conclusion

Many companies have worked to overhaul their supply chain management practices to address risk from vulnerable open source components and third-party commercial software over the past two years. Recent vulnerabilities in widely used software products and open source components appear to be fueling a lot of the change.

A substantial number of organizations in Dark Reading's 2023 Supply Chain Threats Survey have implemented comprehensive controls and recommended best practices — such as maintaining SBOMs and conducting vendor questionnaires — for mitigating supply chain risk. But many more have not implemented these practices and, by their own admission, are a long way from securing their software supply chain. Even so, most IT and security leaders view their organizations as ready to prevent, detect, and respond to supply chain breaches – suggesting a potential disconnect between perception and reality.

Figure 7.



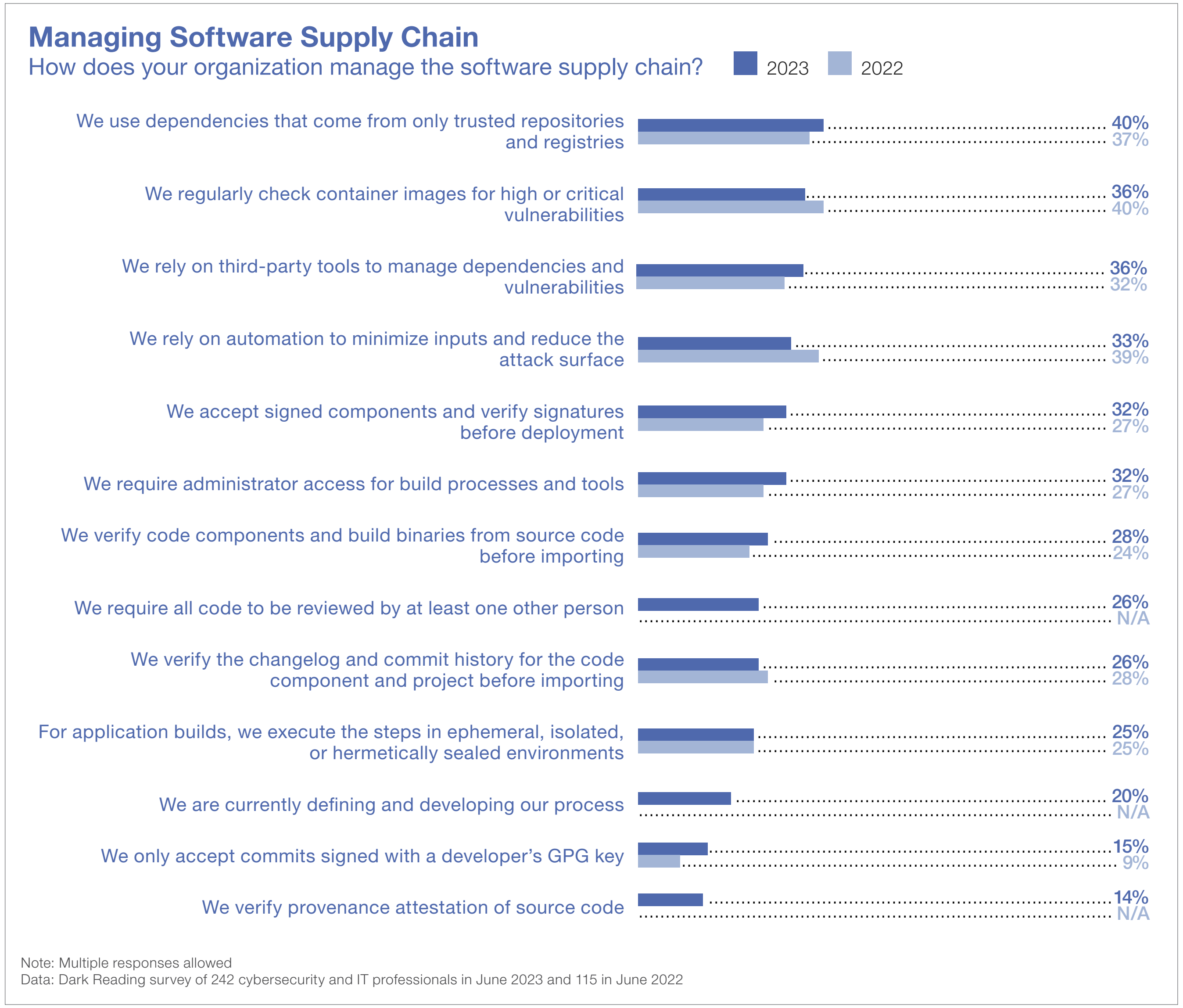
Concerns About Software Supply Chain

Thinking specifically about the software supply chain, please rank the following issues that cause you the most worry from high to low.

	Overall rank	Score
Vulnerabilities in third-party libraries affecting the security of our application	1	800
Developers downloading and importing malicious packages and components	2	724
Attackers tampering with libraries and code repositories to include malicious code	3	602
Software components used in our code, which is no longer being maintained	4	590
Vulnerabilities in build tools and development frameworks used in software development	5	552

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.
Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 8.

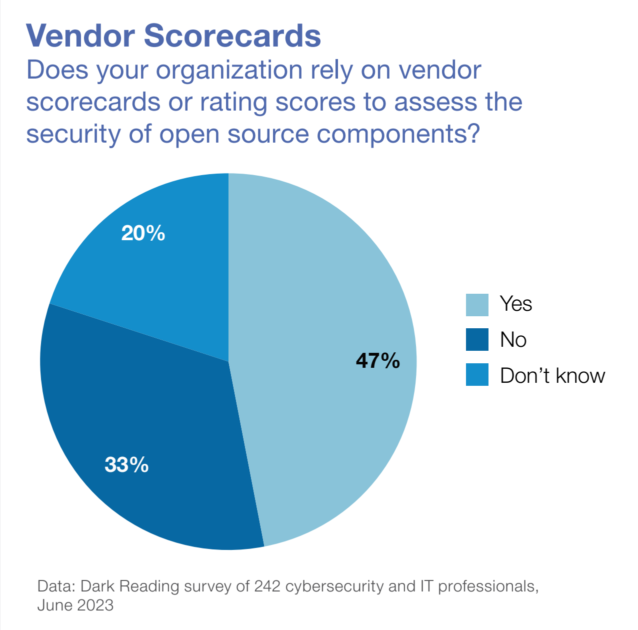


Managing Software Supply Chain

How does your organization manage the software supply chain?

Note: Multiple responses allowed
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Figure 9.



Vendor Scorecards

Does your organization rely on vendor scorecards or rating scores to assess the security of open source components?

Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 10.

Software Bills of Materials

Please tell us how strongly you agree or disagree with the following statements about the software bill of materials.

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
My organization maintains a software bill of materials (SBOM) repository	16%	34%	33%	9%	8%
I believe my organization will increase the use of SBOMs in the next 12 months	18%	30%	41%	8%	3%
My organization uses the SBOM for vulnerability management	13%	28%	37%	12%	10%
My organization regularly requests SBOMs from vendors and suppliers	12%	29%	34%	15%	10%
My organization creates complete SBOMs for all software we build	14%	22%	40%	13%	11%

Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 11.

Build Practices to Prevent Software Supply Chain Attacks

How difficult is it to implement the following build practices and methods for preventing, mitigating, and/or remediating software supply chain security attacks?

	1 - Not difficult at all	2	3	4	5 - Extremely difficult
Using a hermetic build with all inputs declared with immutable references	2%	10%	45%	27%	16%
Making provenance information (when/where/how the software was produced) available	3%	19%	46%	19%	13%
All build steps must be run on a build service — not locally on a developer's workstation	8%	14%	51%	20%	7%
Re-running builds with the same input artifacts must result in bit-by-bit identical output	6%	15%	52%	19%	8%
Running builds in an ephemeral environment, such as a container or virtual machine, or in an isolated environment	6%	23%	47%	14%	10%

Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 12.

Software Supply Chain Statements

Please tell us how strongly you agree or disagree with the following statements about the software supply chain.

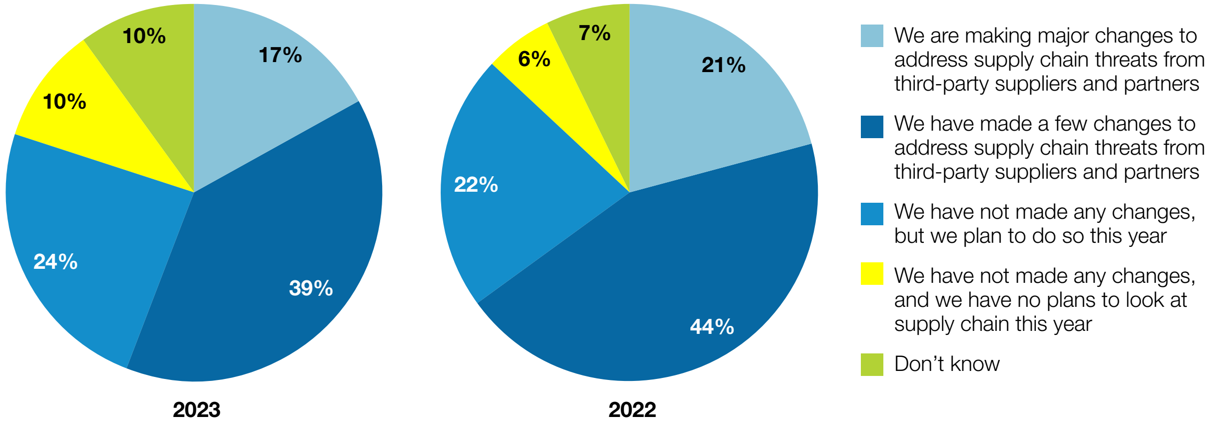
	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
My organization will be able to detect and respond to a software supply chain compromise	18%	46%	27%	8%	1%
“Shifting left” is necessary to secure the software supply chain	20%	35%	40%	4%	1%
I believe our architects and developers have the necessary knowledge and expertise to ensure a secure software supply chain	23%	30%	31%	13%	3%
My organization has a way to detect software tampering across the software supply chain	19%	32%	31%	12%	6%

Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 13.

Effect of Recent Attacks on Organizations’ Approach to Supply Chain Security

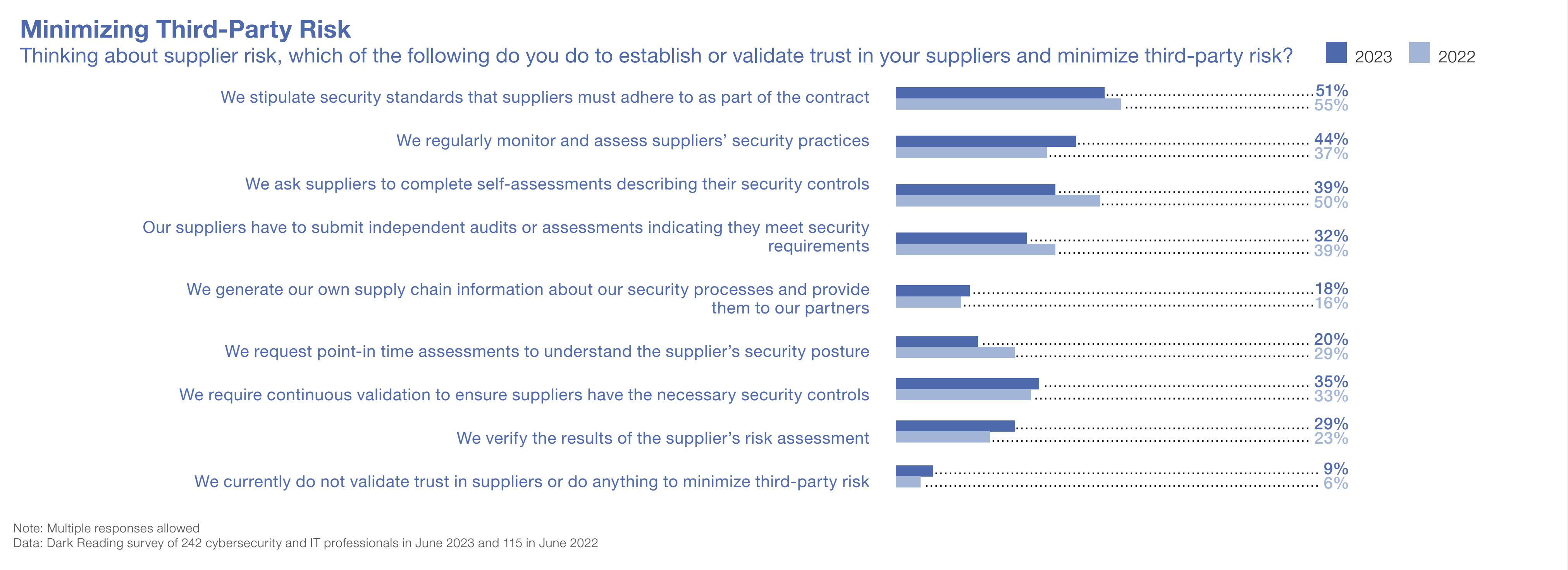
How have attacks against trusted third-party software — such as Microsoft Exchange, Kaseya, and Accellion — changed your organization’s approach to supply chain security?



Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Previous Next
Table of Contents

Figure 14.



Minimizing Third-Party Risk

Thinking about supplier risk, which of the following do you do to establish or validate trust in your suppliers and minimize third-party risk?

Note: Multiple responses allowed
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

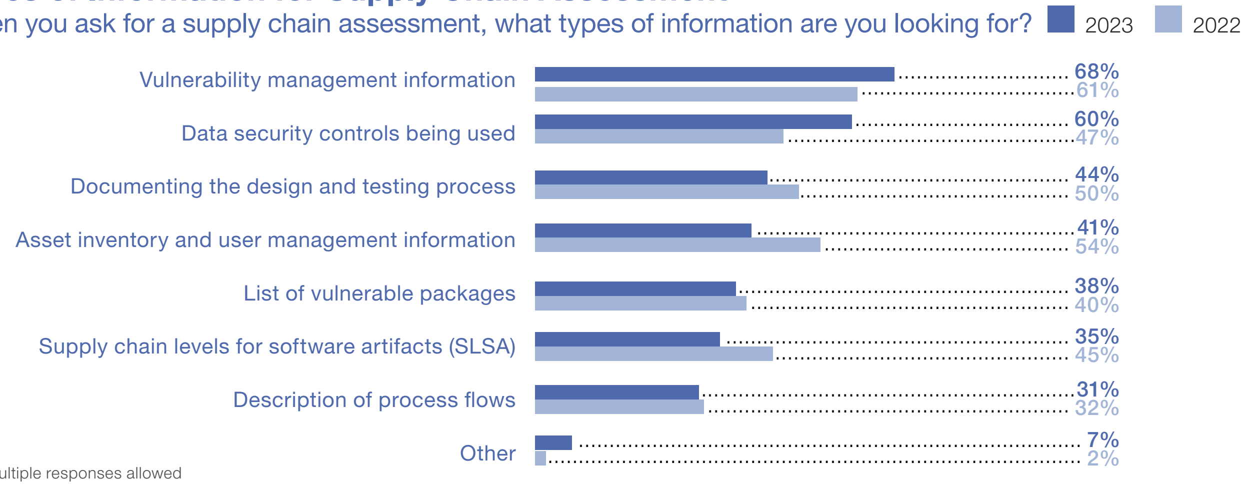
Previous Next

Table of Contents

Figure 15.

Types of Information for Supply Chain Assessment

When you ask for a supply chain assessment, what types of information are you looking for?

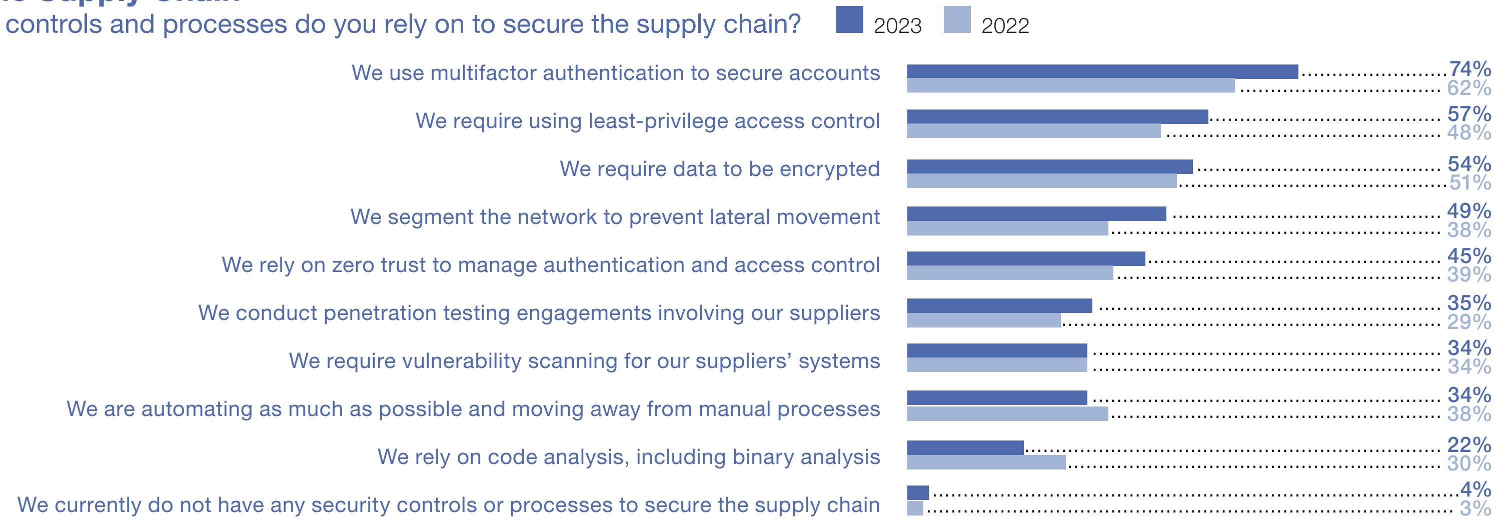


Note: Multiple responses allowed
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Figure 16.

Securing the Supply Chain

What security controls and processes do you rely on to secure the supply chain?



Note: Multiple responses allowed
Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

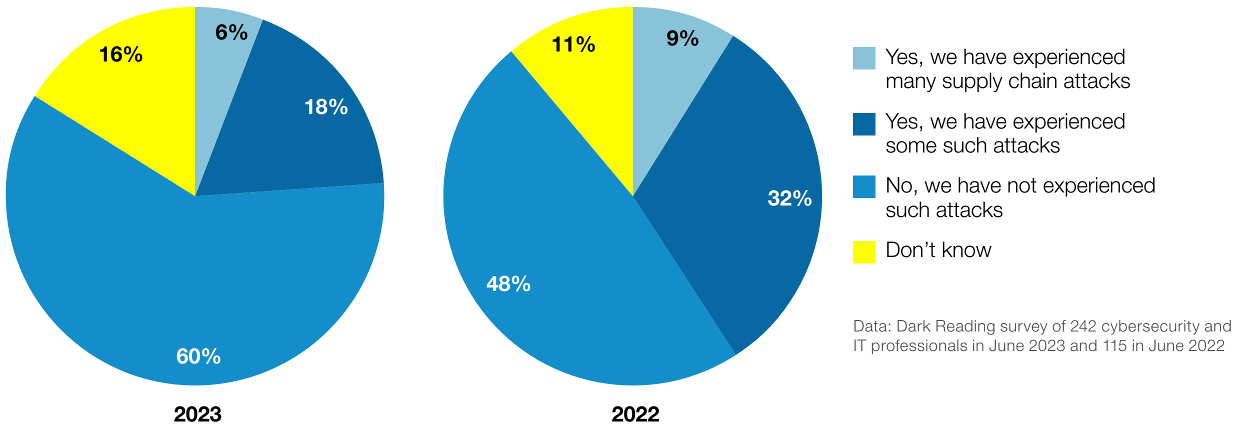
Previous Next

Table of Contents

Figure 17.

Supply Chain Attack

Has your organization experienced any kind of supply chain attacks over the past year?

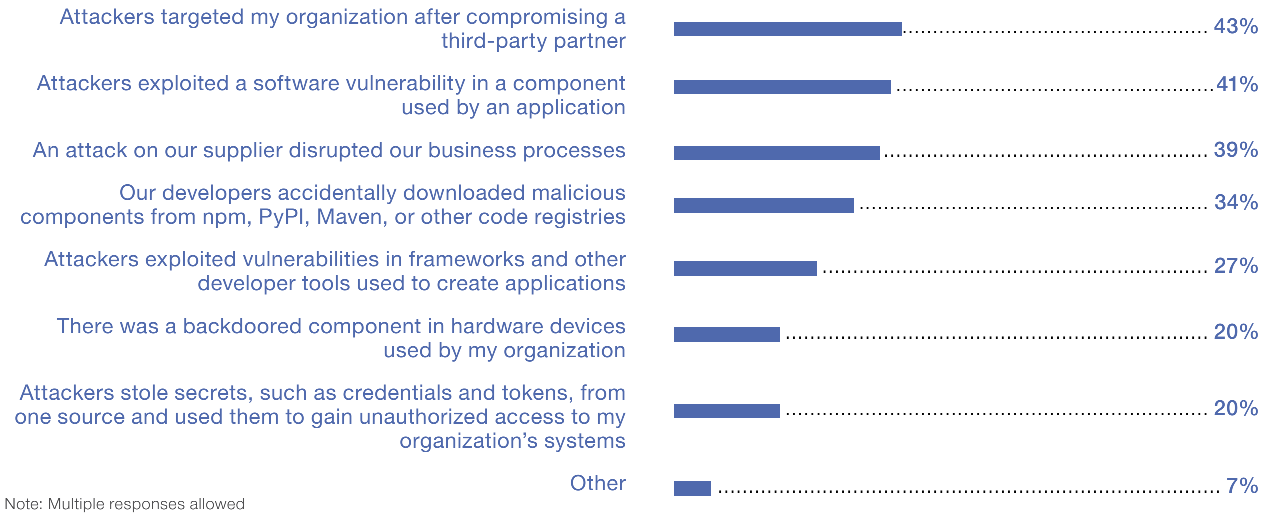


Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

Figure 18.

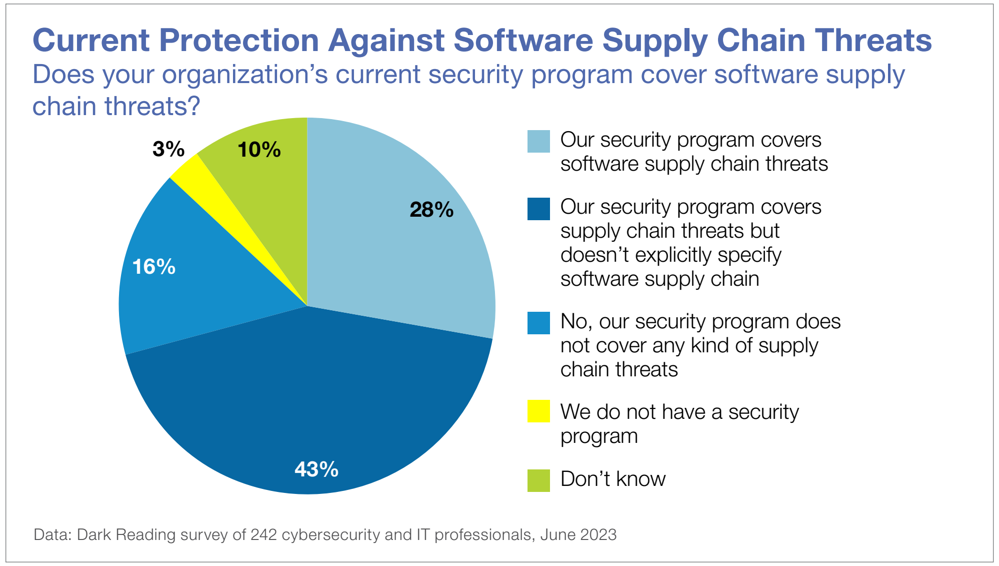
Types of Attacks

Which types of supply chain attacks did your organization experience over the past year?



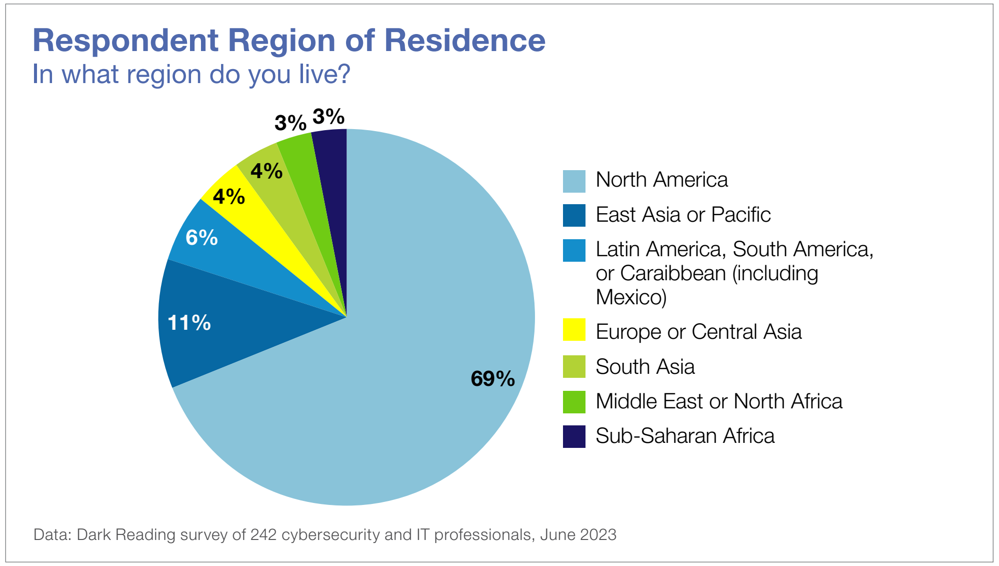
Note: Multiple responses allowed
Base: 58 respondents who have experienced supply chain attacks
Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 19.



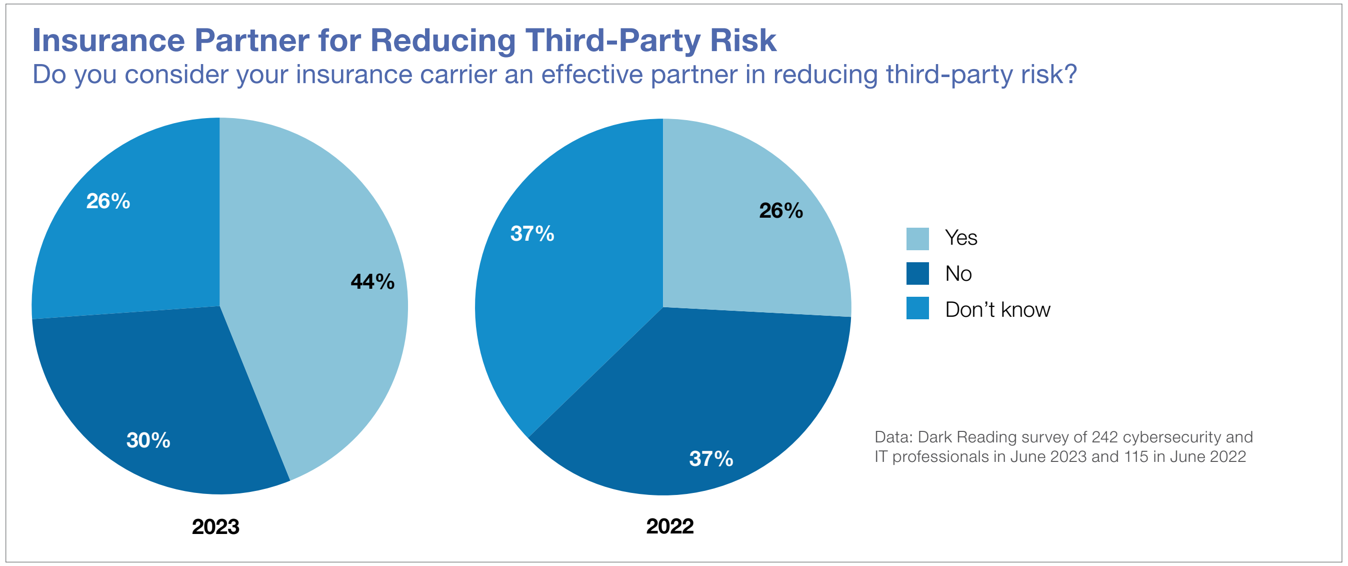
Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 21.



Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 20.



Data: Dark Reading survey of 242 cybersecurity and IT professionals in June 2023 and 115 in June 2022

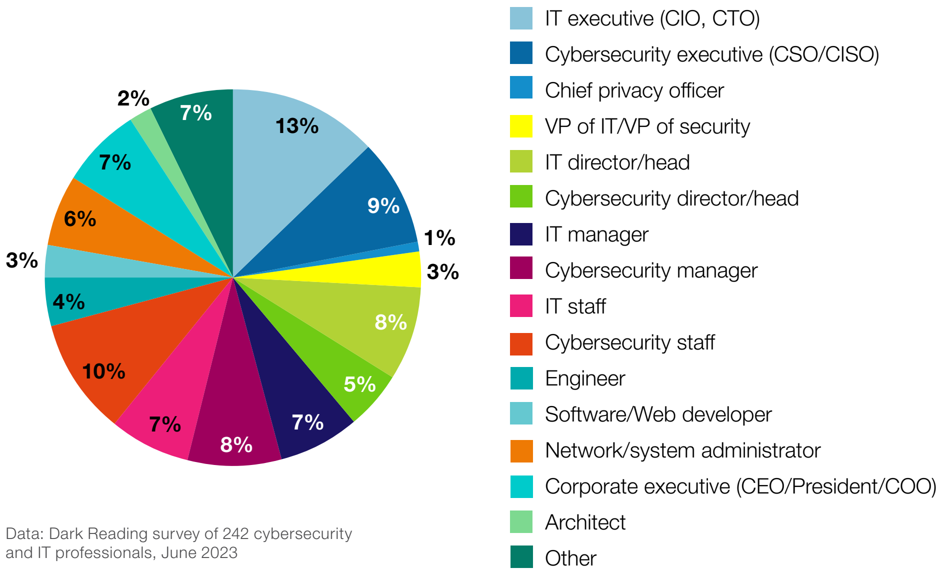
Previous

Table of Contents

Figure 22.

Respondent Job Title

Which of the following best describes your job title?

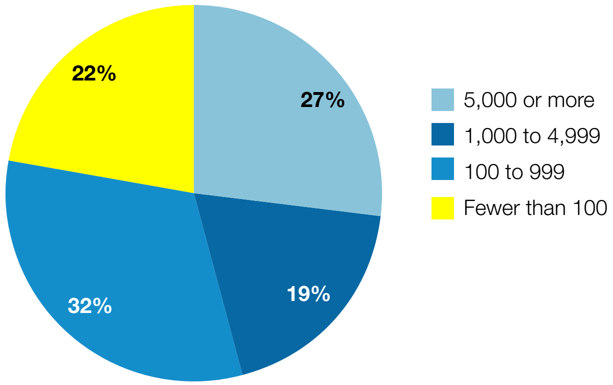


Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 23.

Respondent Company Size

How many employees are in your company in total?

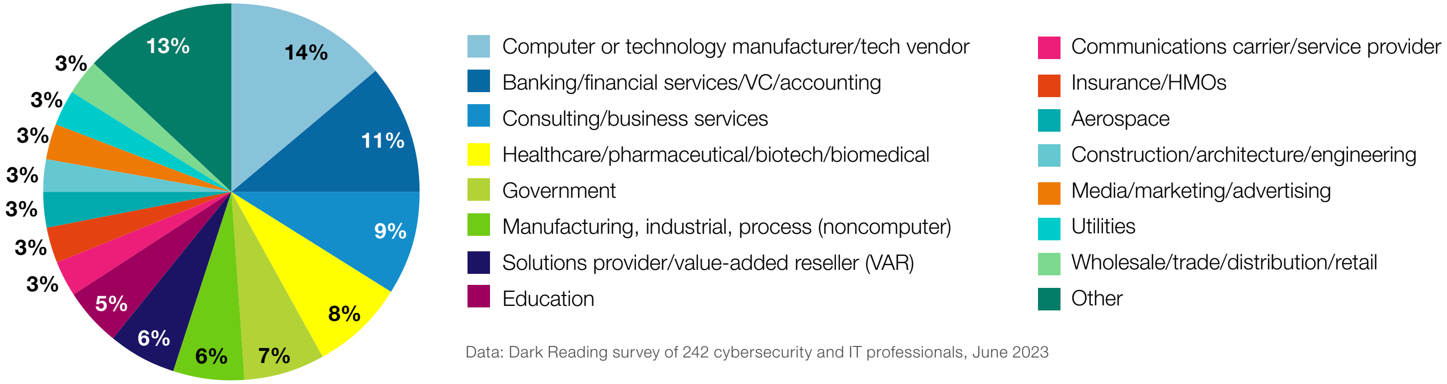


Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023

Figure 24.

Respondent Industry

What is your organization's primary industry?



Data: Dark Reading survey of 242 cybersecurity and IT professionals, June 2023