BlackBerry | Cybersecurity

Software Supply Chain Research

Christine Gadsby
Vice President & CISO, Cybersecurity

May 2024

Coleman Parkes

Study Detail

Methodology
Online survey

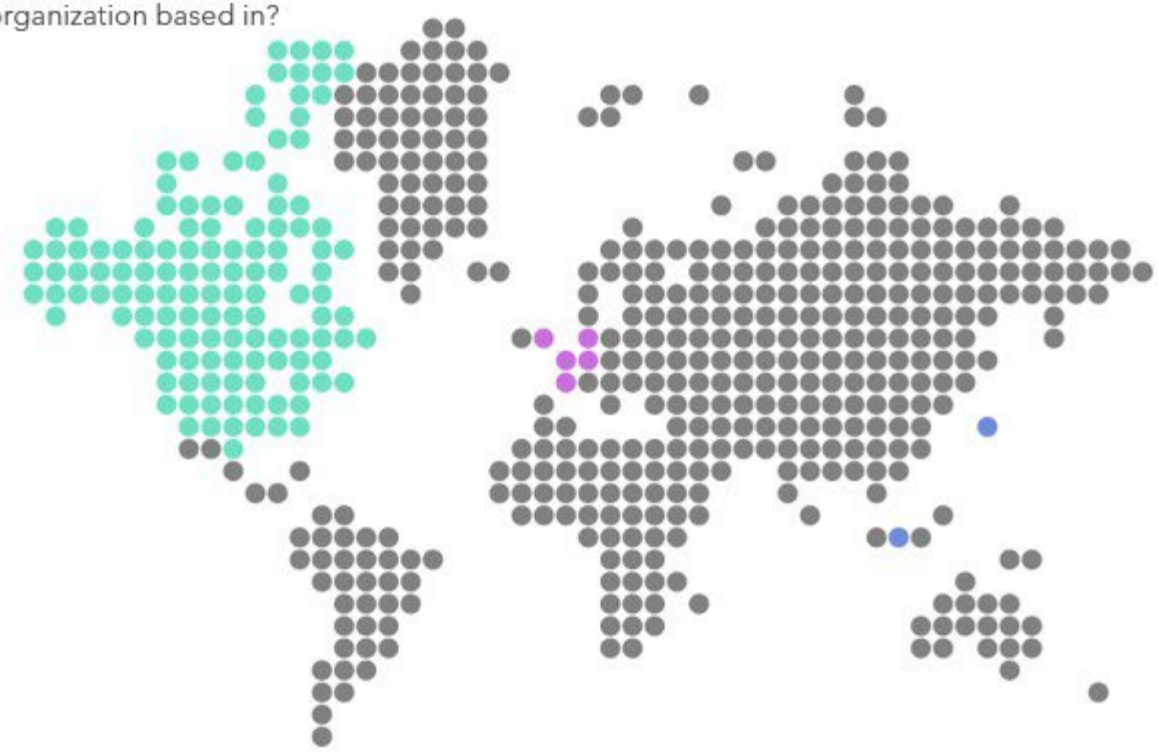
Audience Profile
Senior ITDM's and Cybersecurity leaders with an understanding of the procedures to manage risk of security breaches from supply chains

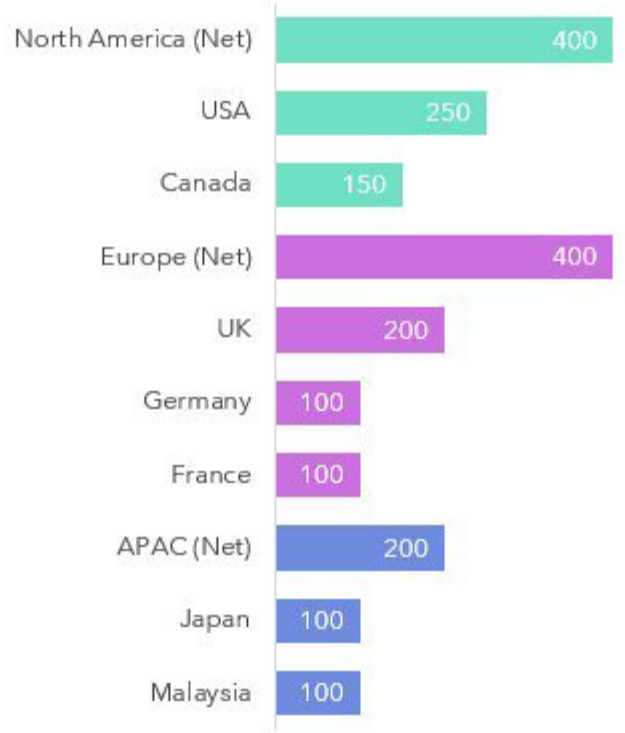
Fieldwork Dates
March - April 2024

Number of interviews

North America: 400
Europe: 400
APAC: 200

S1. Which country is your organization based in?



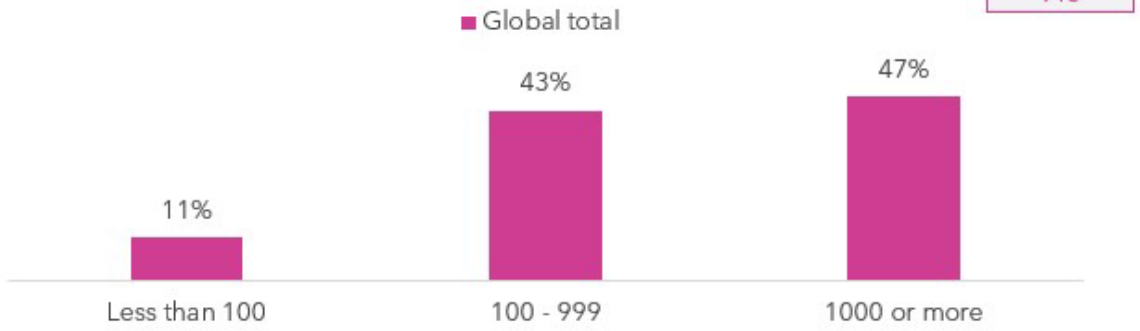


Annual revenue

S3. In USD$, what was your organization's annual revenue (or equivalent) for the current financial year?

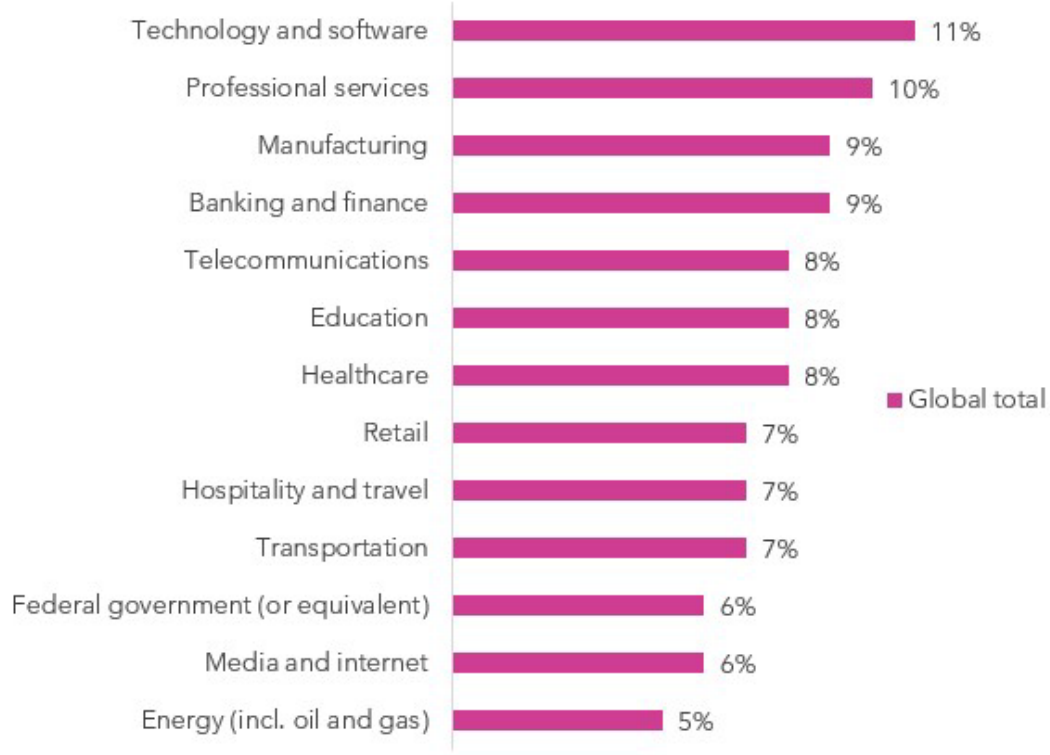
Number of employees

S4. How many employees does your organization have?



Sector

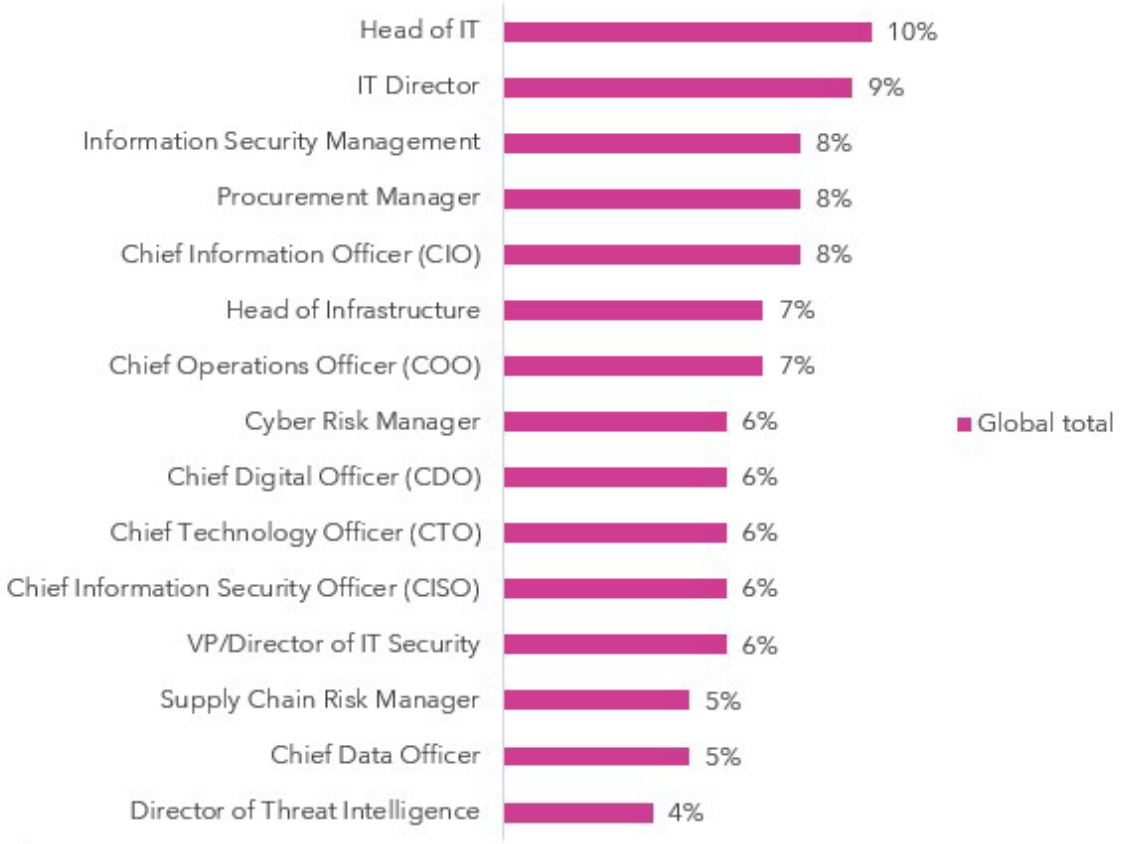
Q.S2. In which sector does your organization operate in primarily?



Base: Global total (1,000)

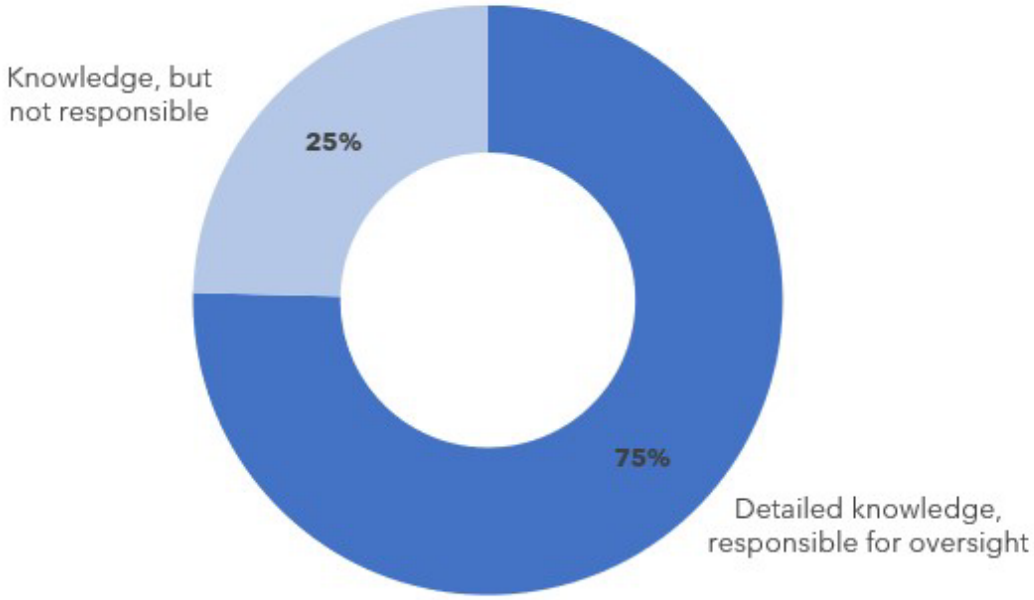
Job title

S5. Which of these titles is the closest to your role?



Knowledge of procedures to manage/ mitigate security breaches

S6. Does your role entail that you have knowledge or oversight of the procedures in place to manage and mitigate risk of security breaches from supply chains used by your organization?

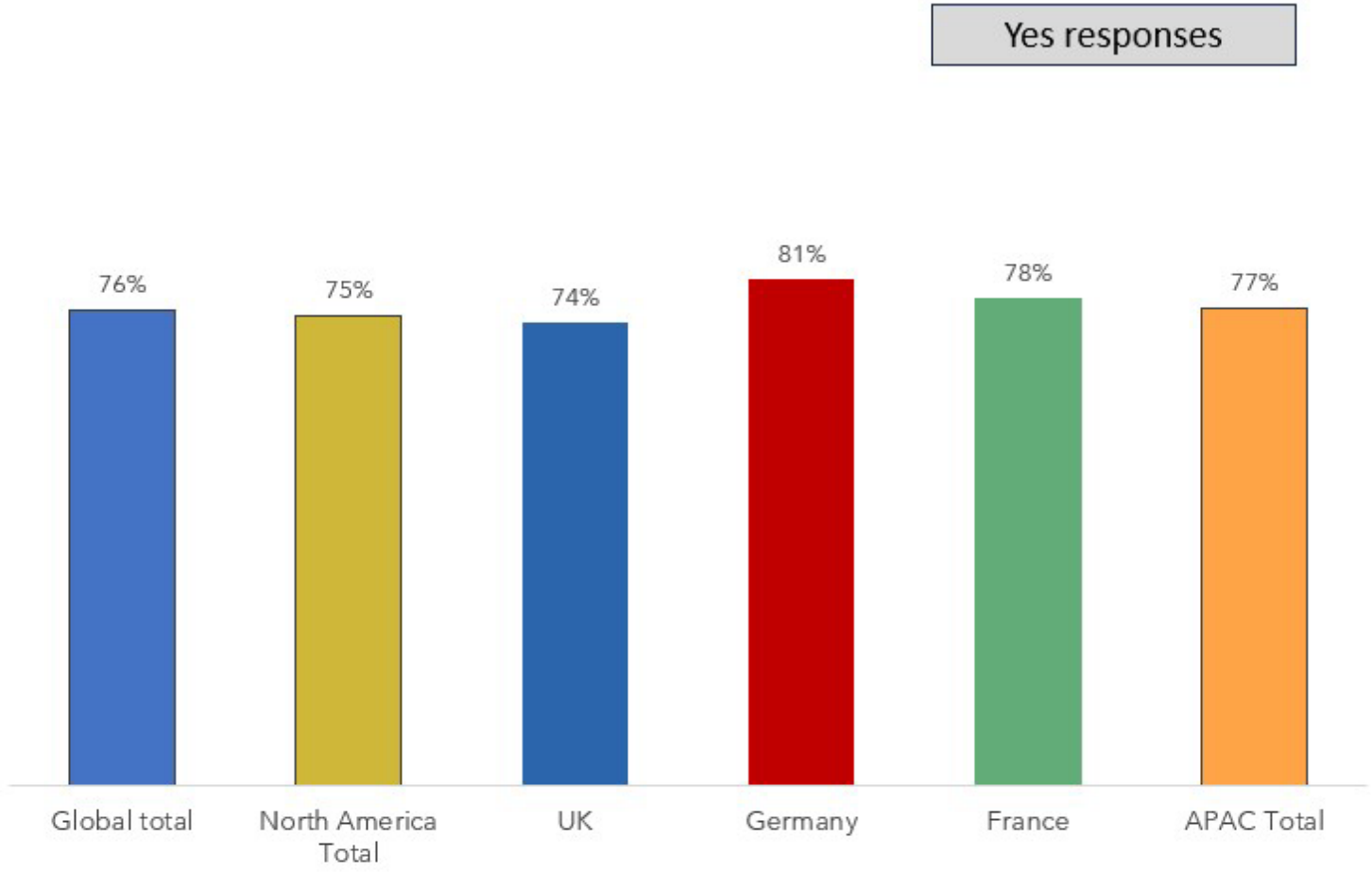


Base: Global total (1,000)

Section 1

Working With Suppliers and Partners To Secure the Supply Chain of Software You Consume

Being notified of a vulnerability or attack within software supply chain in the last 12 months

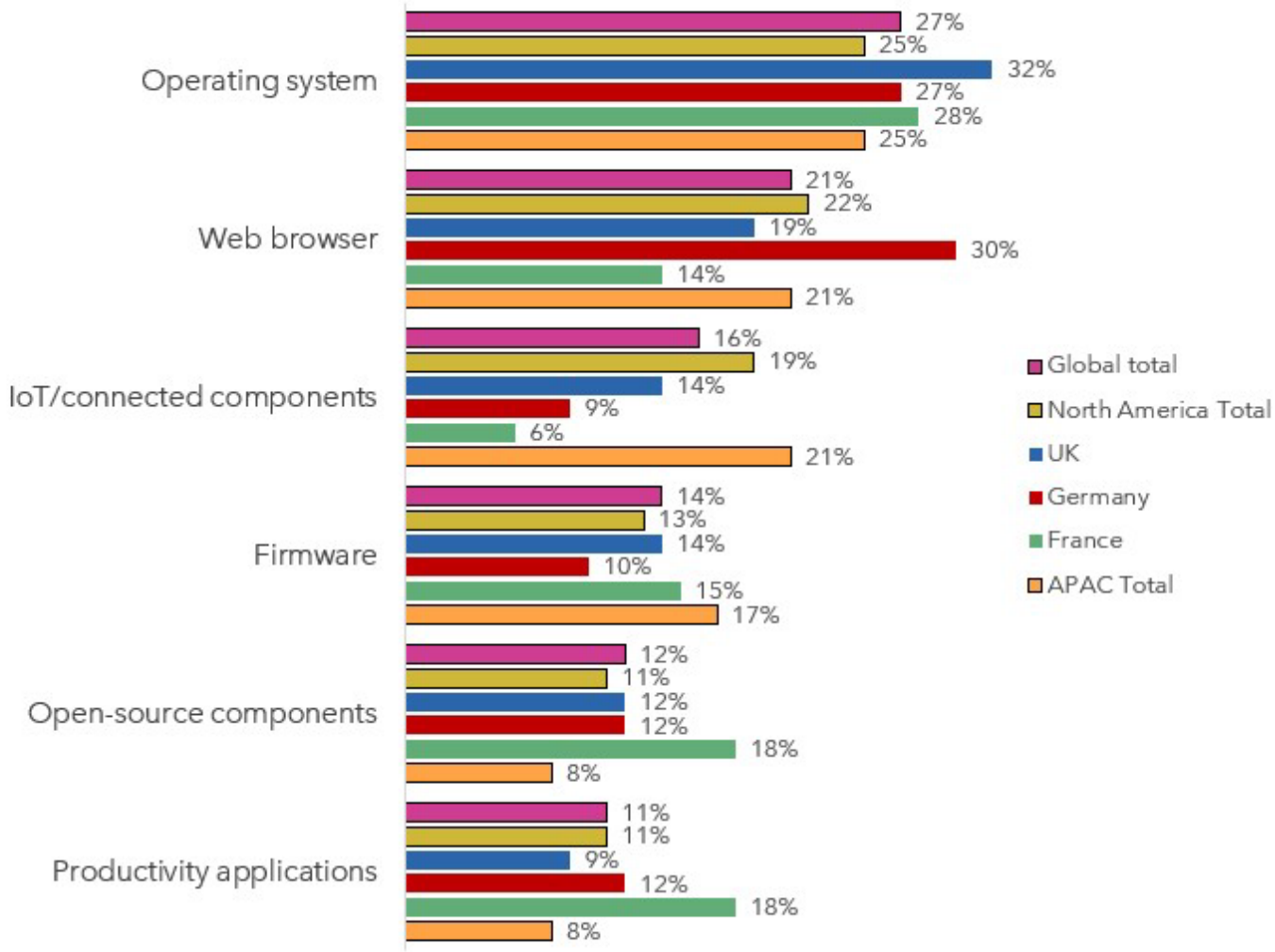


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q1. Has your organization been notified of a vulnerability or attack within the supply chain of software you consume in the last 12 months?

Vulnerable components having the biggest impact for organization

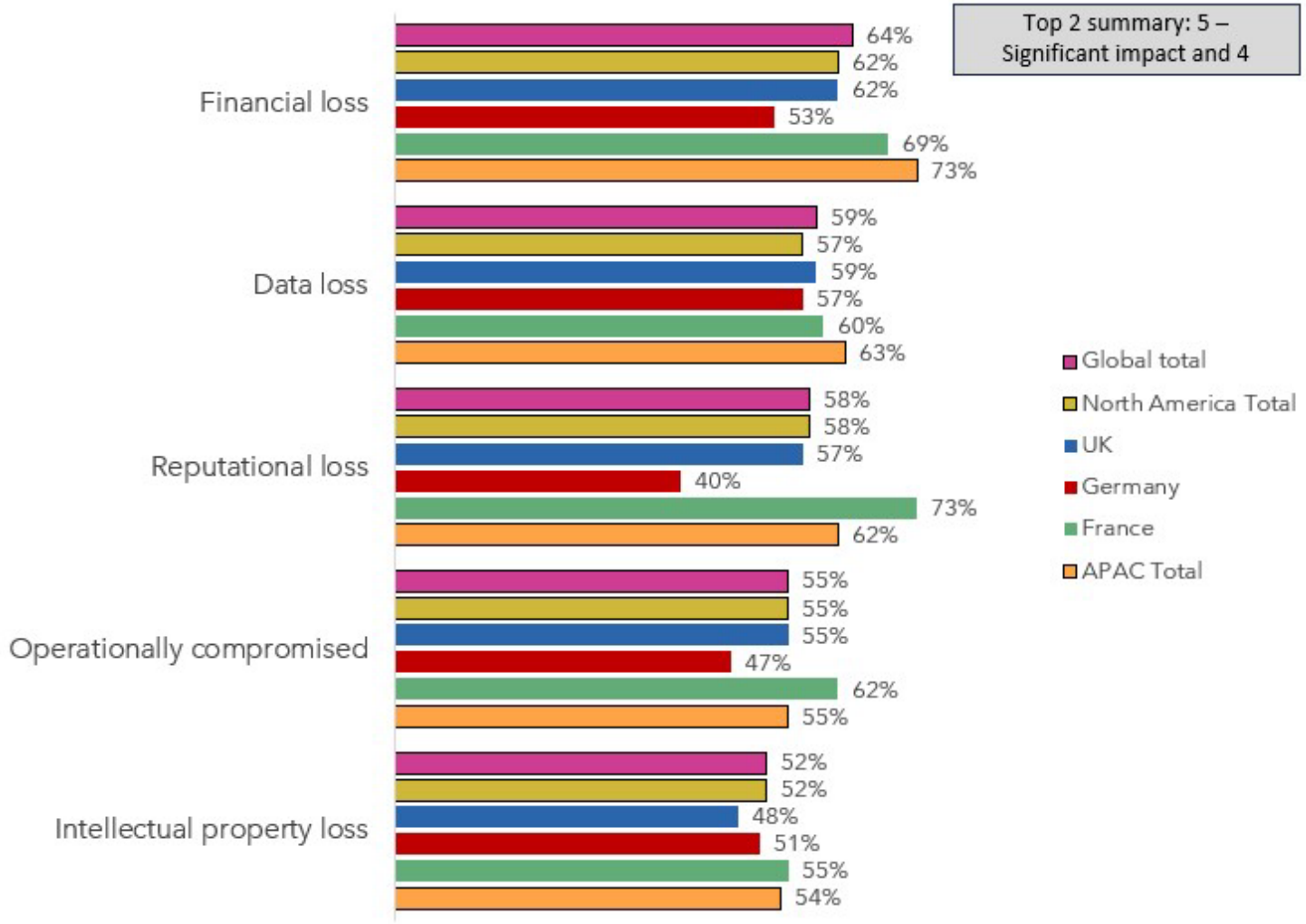


Base: Respondents who have been notified of a vulnerability or attack within their supply chain (761) North America (301) UK (148) Germany (81) France (78) APAC total (153)

Single coded question

Q2. Which of the following vulnerable components, resulted in the biggest impact for your organization?

Significance of the attack on the business

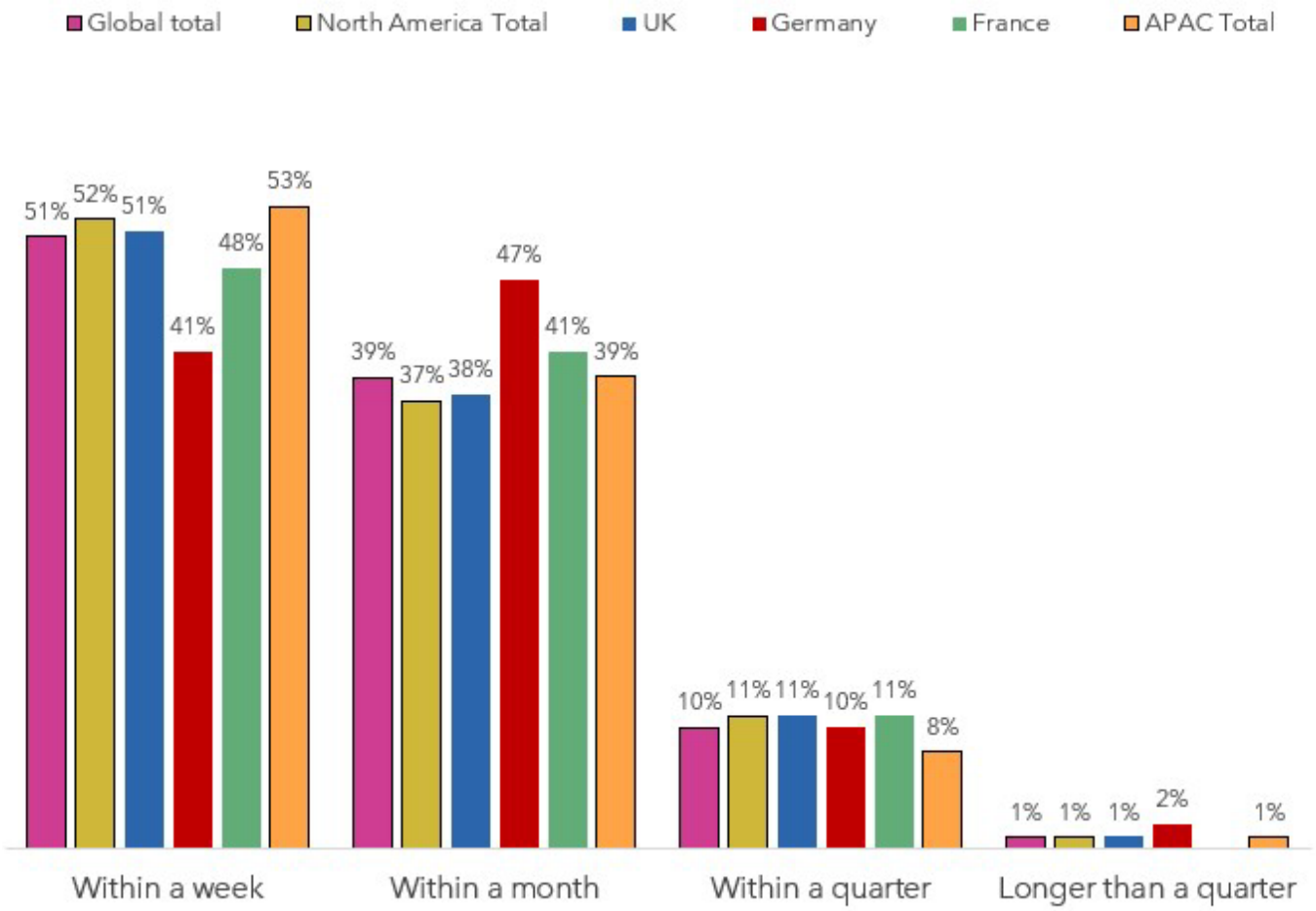


Base: Respondents who have been notified of a vulnerability or attack within their supply chain (761) North America (301) UK (148) Germany (81) France (78) APAC total (153)

Single code per option

Q3. How significant was the impact of the attack on each of the below?

Time taken to fully recover from an exploited vulnerability in software supply chain

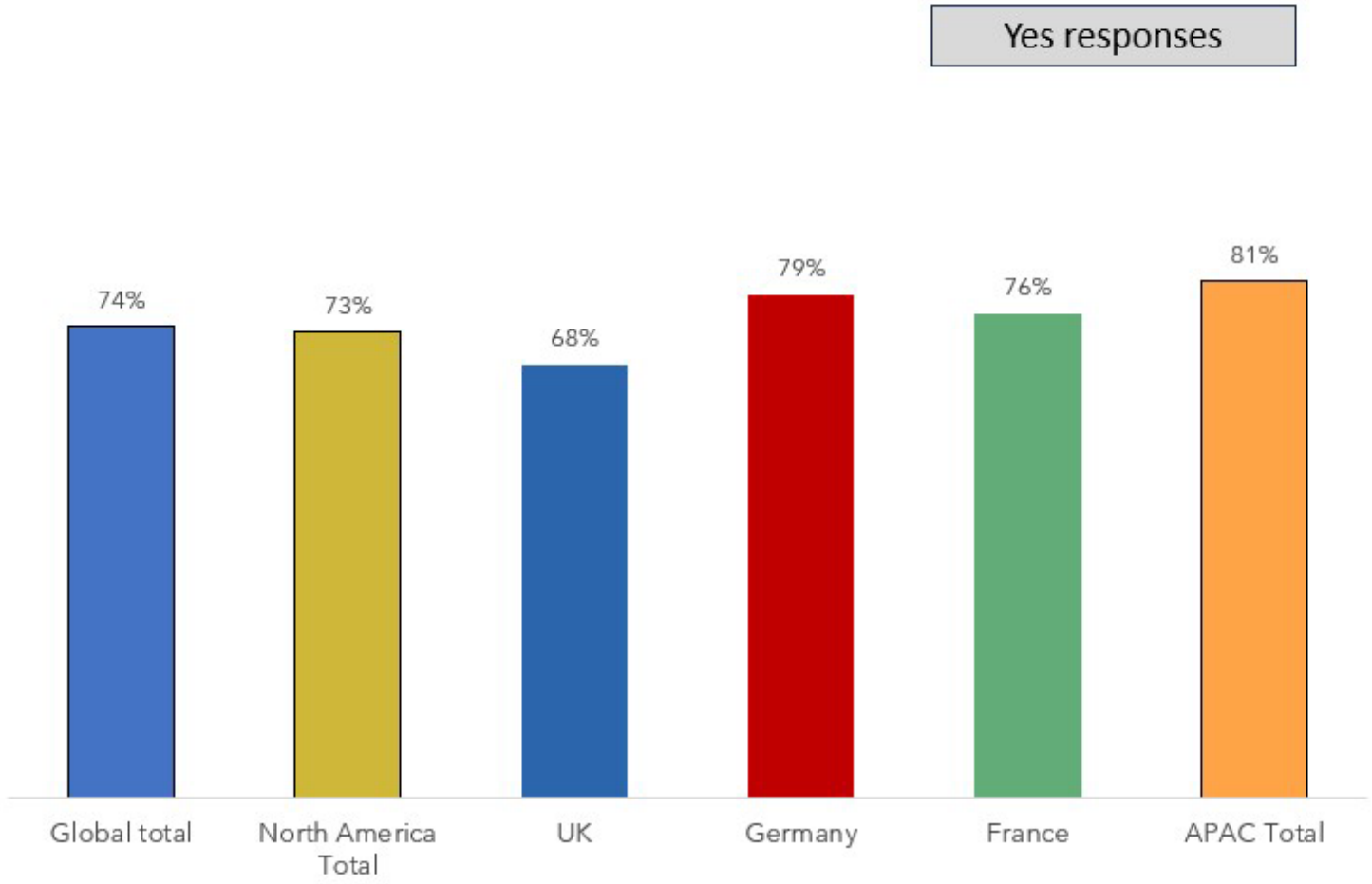


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q4. On average, how long does it take to fully recover from an exploited vulnerability in your software supply chain?

Made aware of a member of supply chain not previously aware of / monitoring for security practices

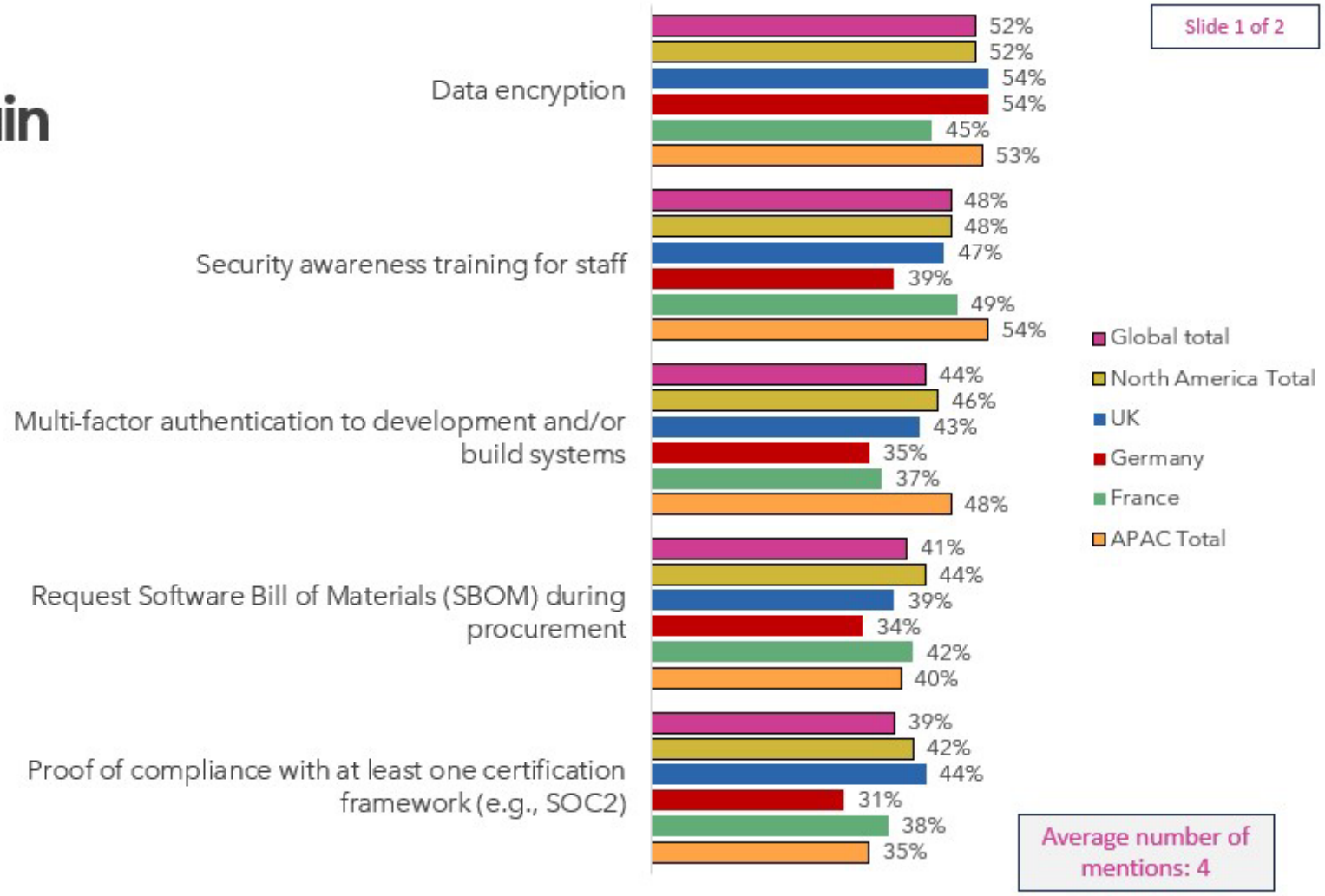


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q5. Over the last year, have you been made aware of a member of your supply chain that you weren't previously aware of / monitoring for security practices?

Measures insist supply chain has in place

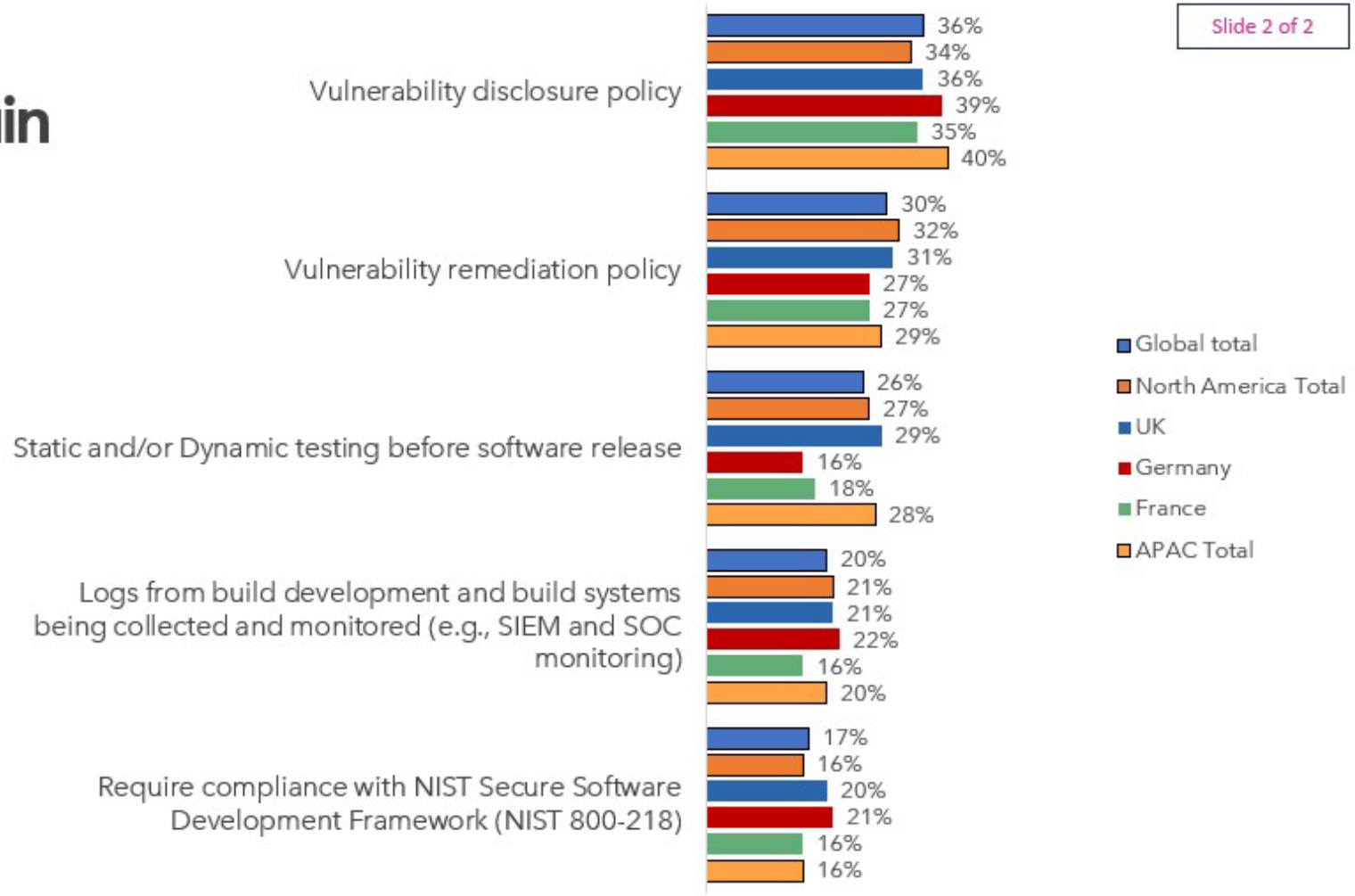


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Multi coded question

Q6. What measures do you insist that your supply chain has in place?

Measures insist supply chain has in place

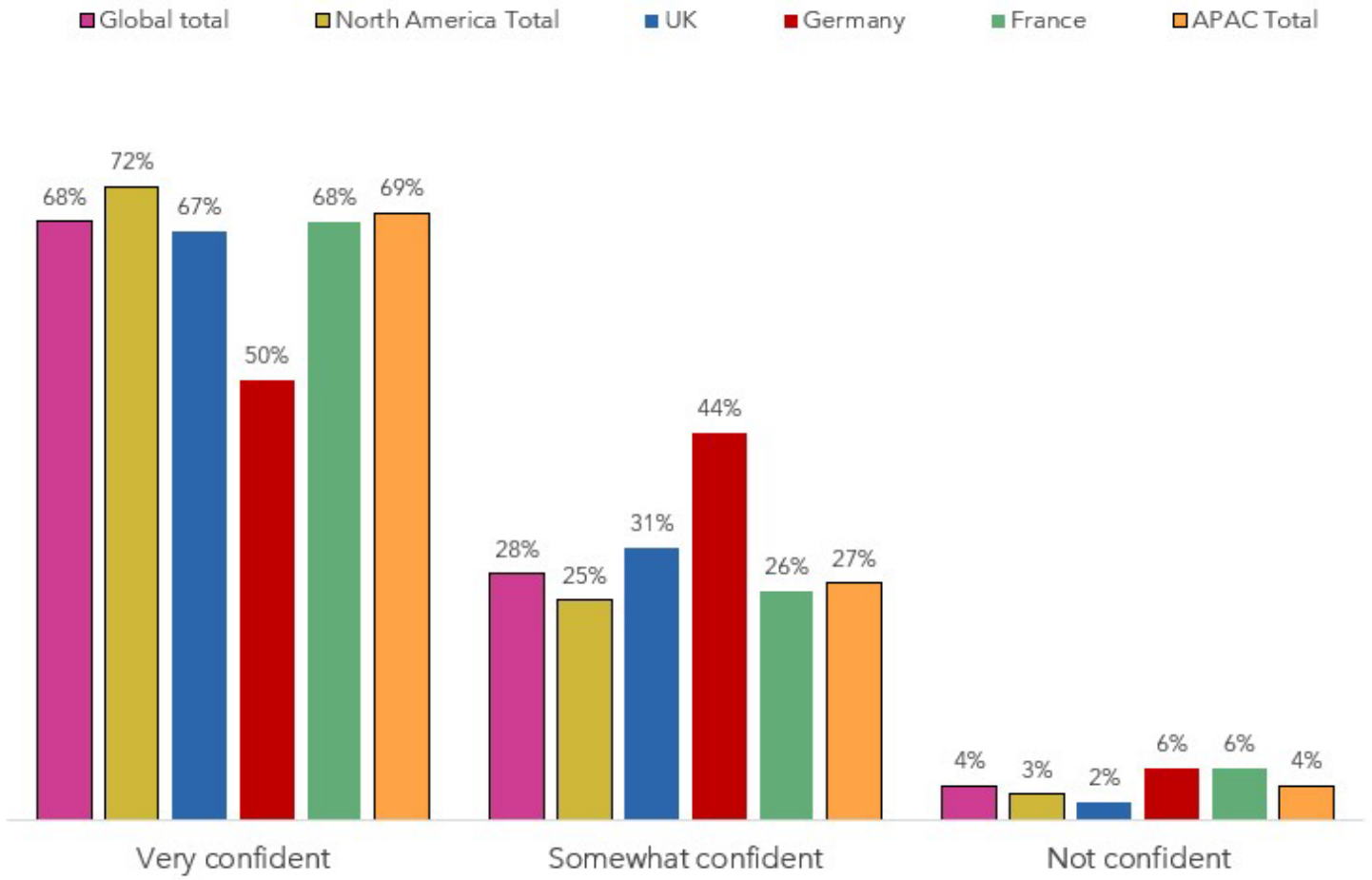


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Multi coded question

Q6. What measures do you insist that your supply chain has in place?

Confidence that suppliers / partners can identify and prevent a vulnerability

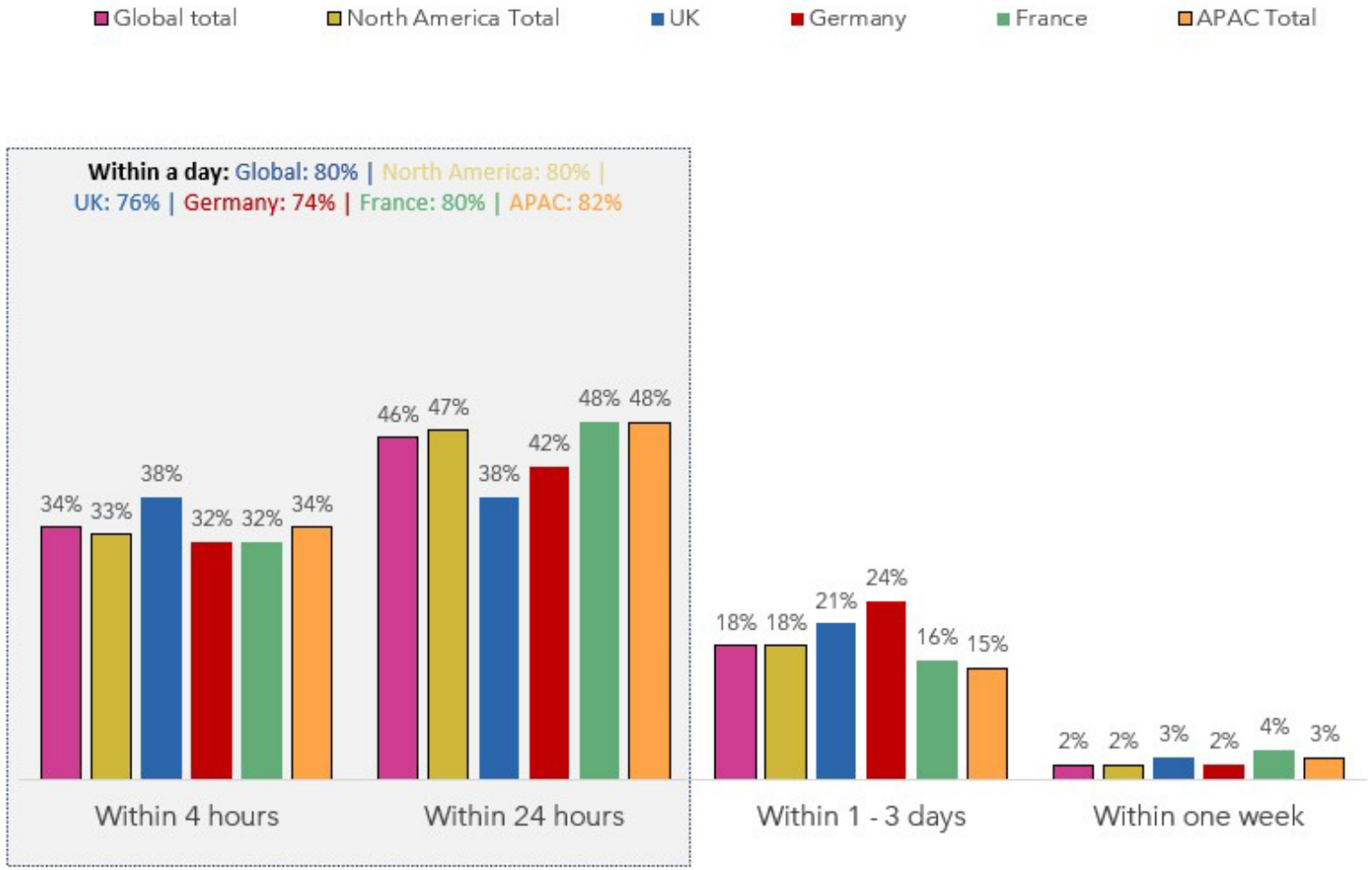


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q7. How confident are you that your suppliers / partners can identify and prevent exploit of a vulnerability within their environment?

Expected time taken to be notified in the event of a supplier / partner suffering a cyber breach

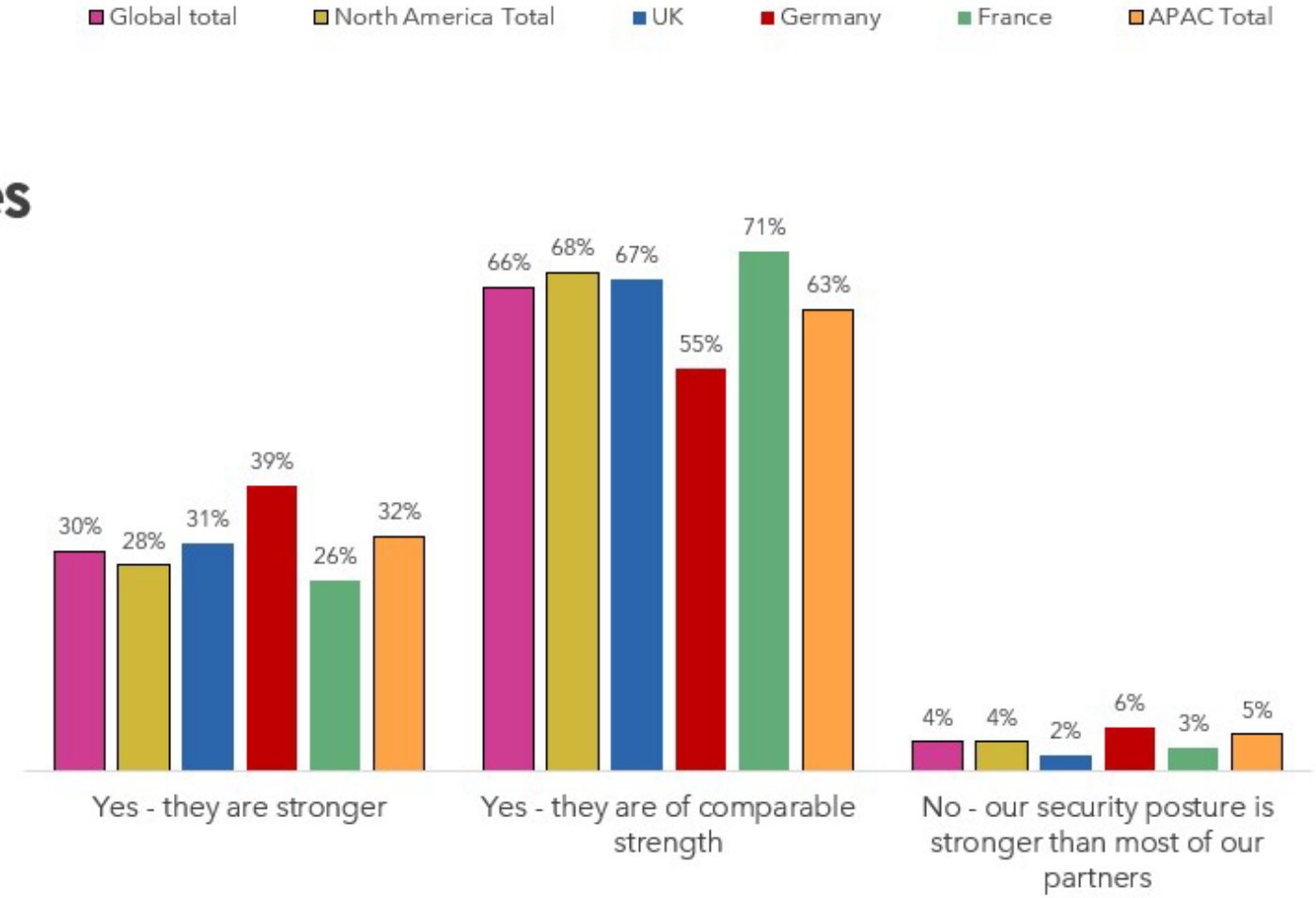


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q8. How quickly do you expect to be notified in the event of a supplier / partner within your software supply chain suffering a cyber breach?

Comparability of suppliers / partners cybersecurity policies

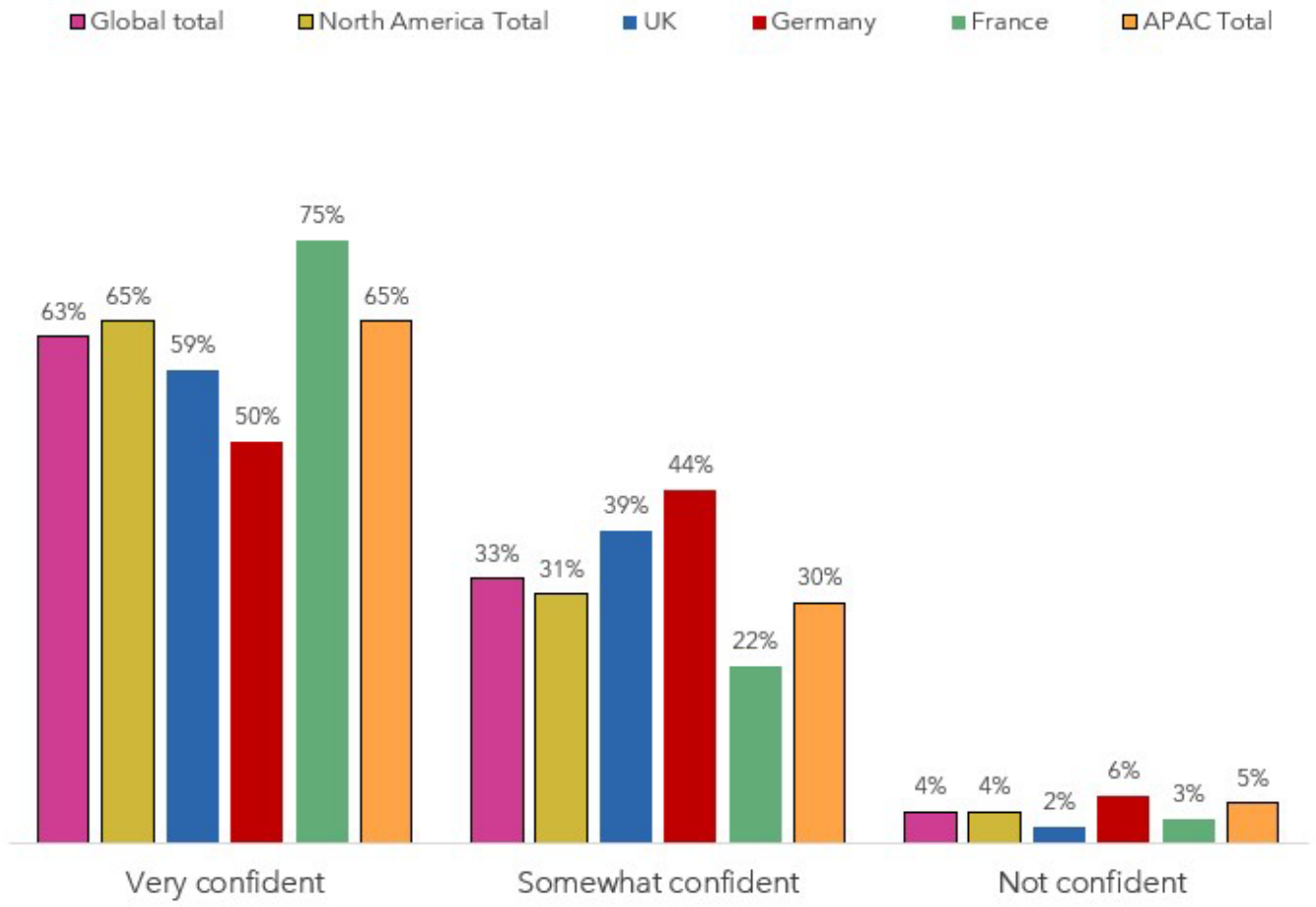


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q9. Do you believe the suppliers / partners of your software supply chain cybersecurity policies are comparable to those implemented at your company?

Confidence that suppliers / supply chain partners have adequate cybersecurity regulatory and compliance practice

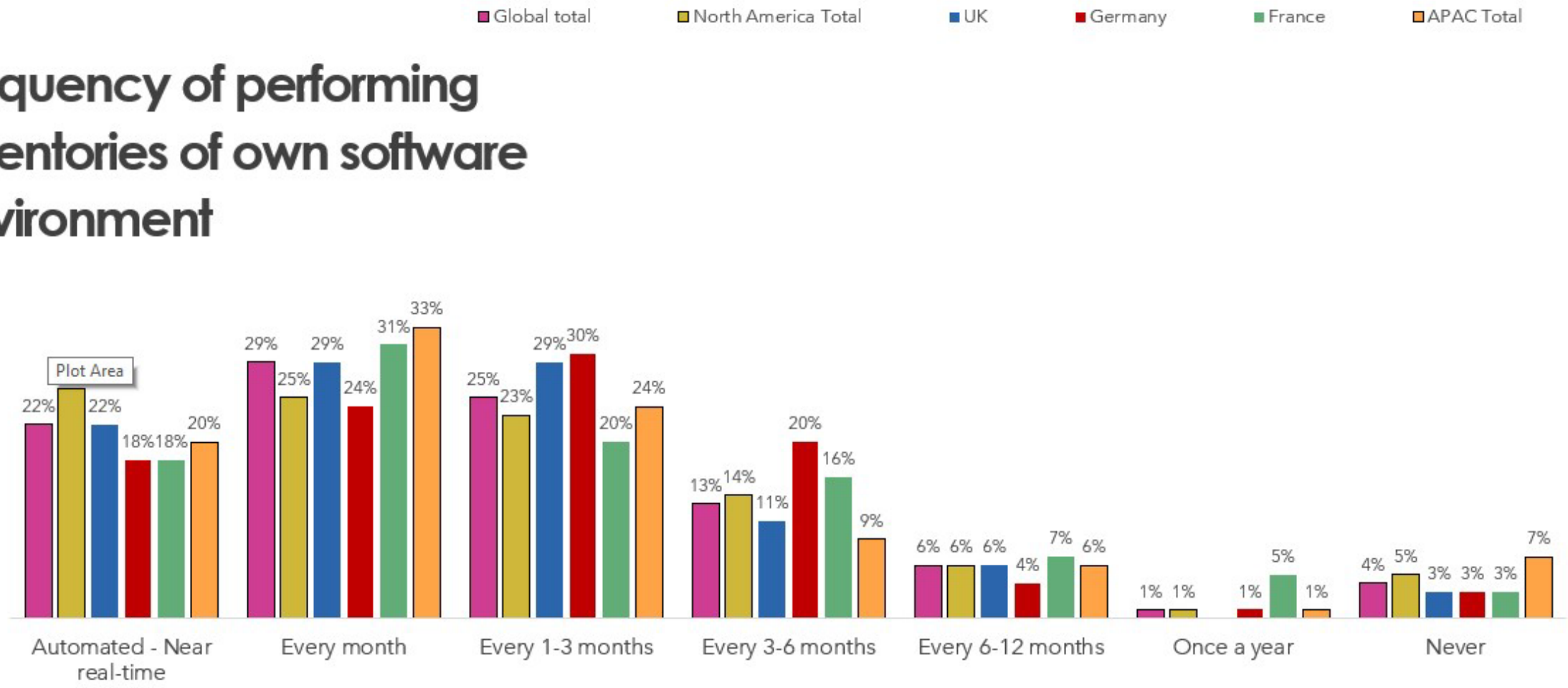


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q10. How confident are you that your suppliers / supply chain partners have adequate cybersecurity regulatory and compliance practice?

Frequency of performing inventories of own software environment

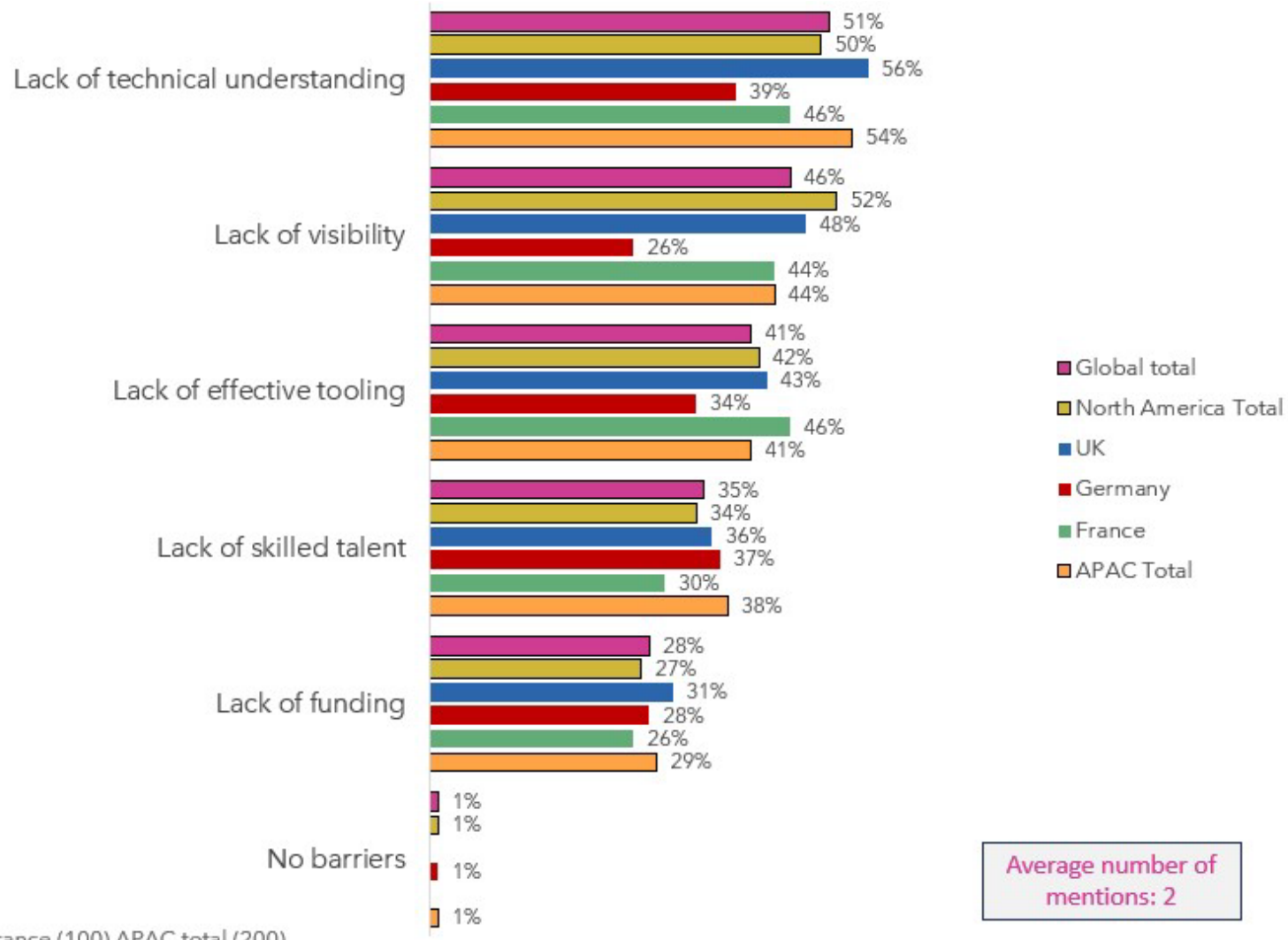


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q12. How often do you perform an inventory of your own software environment?

Biggest barriers to regular software inventories

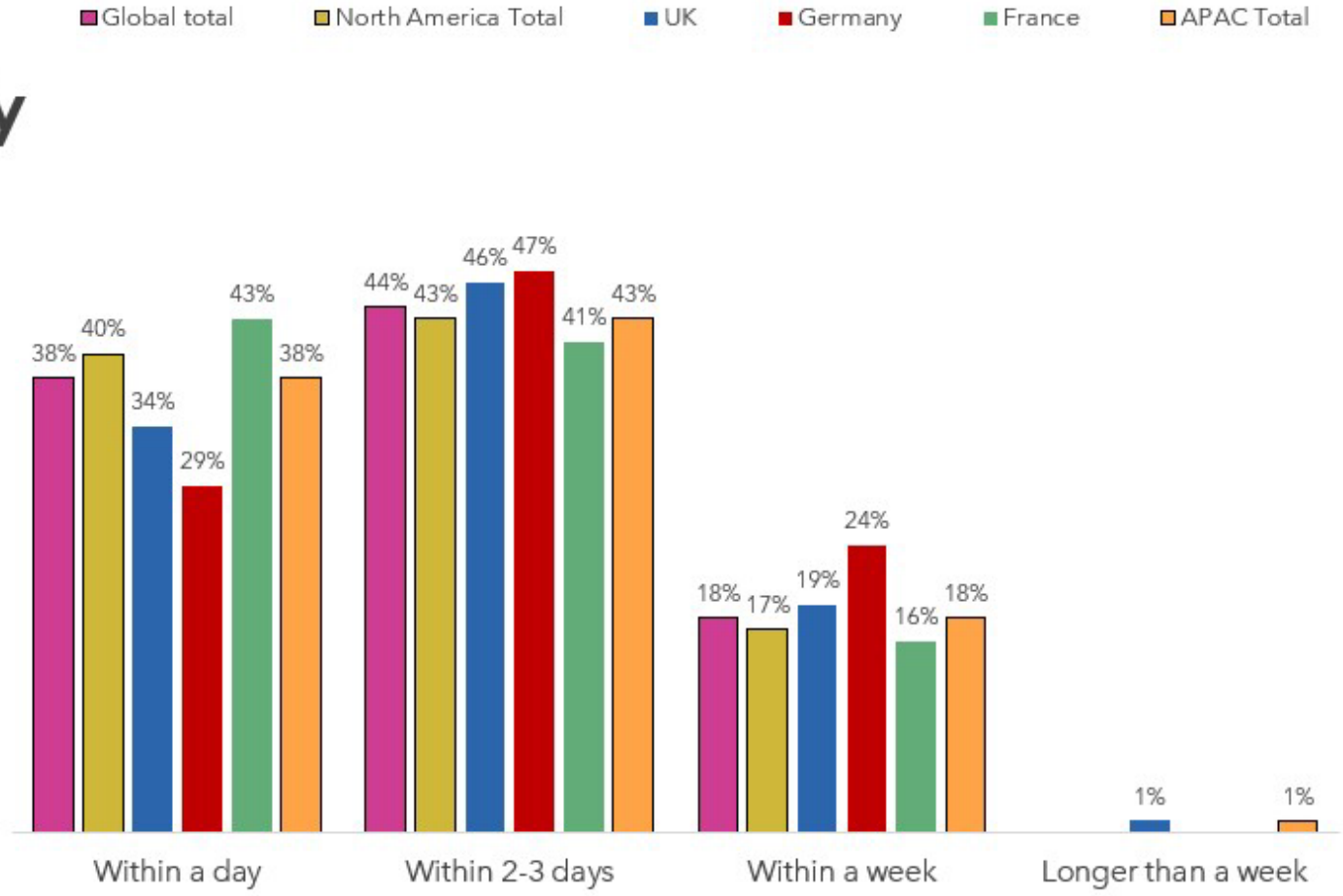


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Multi coded question

Q13. What are the biggest barriers to regular software inventories?

Average time taken to identify if an impacted library is used following a vulnerability

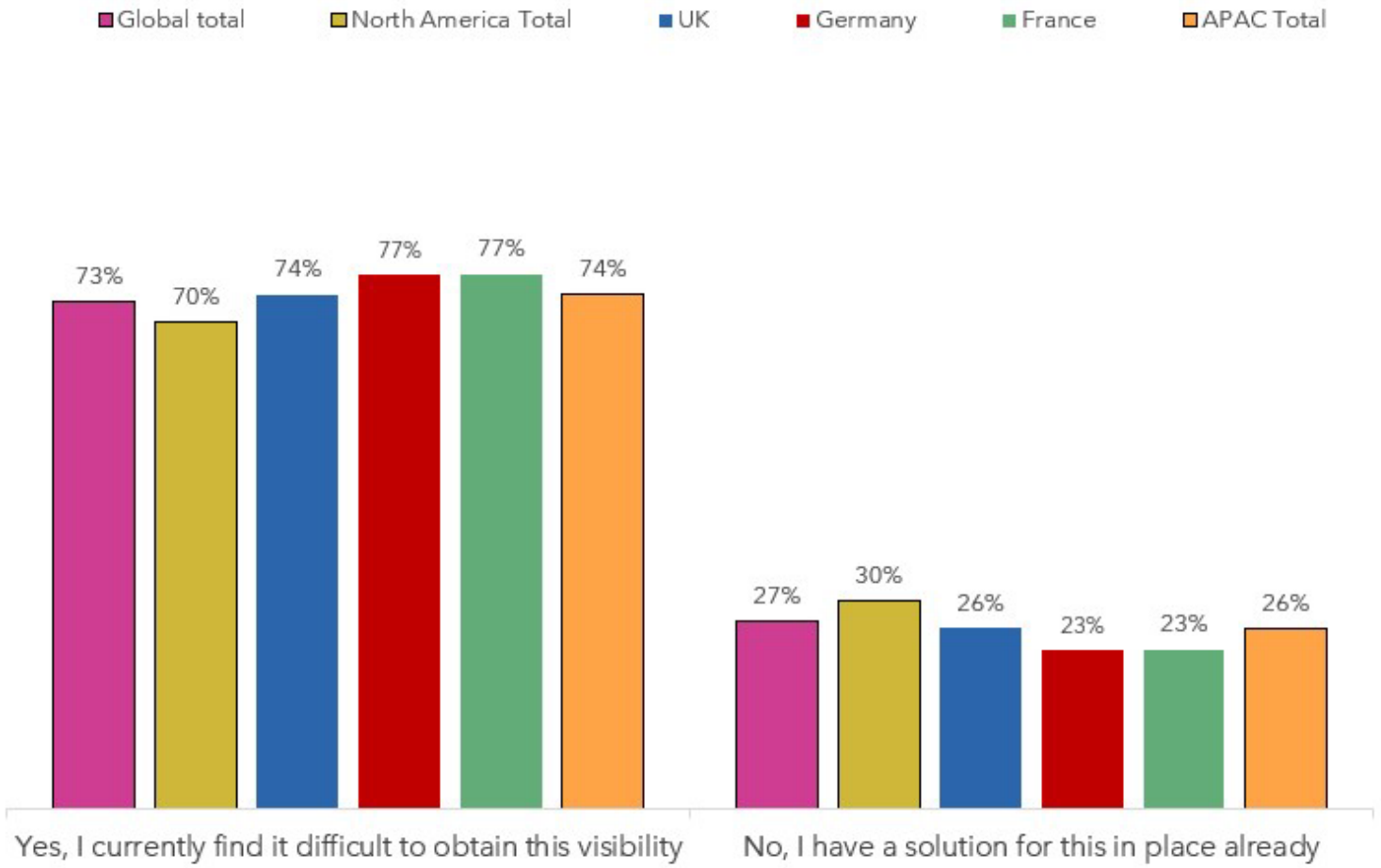


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q14. You have become aware of a vulnerability that may impact the supply chain of software you consume. From the time you start your investigation, on average, how long does it take your organization to identify if an impacted library is used in any of the software you consume?

Usefulness of tool to inventory software libraries and bring greater visibility to software impacted by a vulnerability



Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

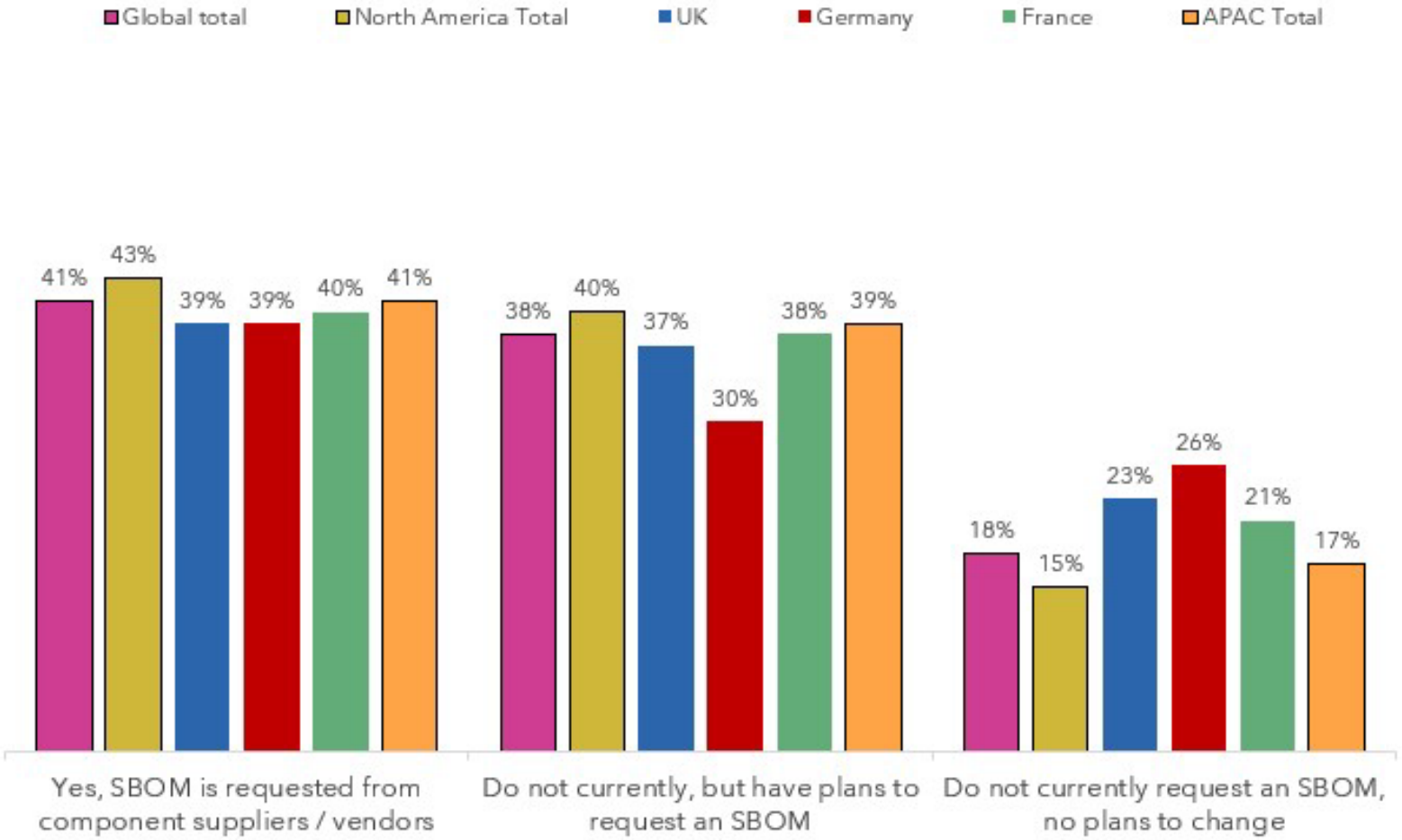
Q15. Would you find a tool that could inventory software libraries within your supply chain and bring greater visibility to software impacted by a vulnerability useful?

Section 2

Regulations and Compliance

Requests for a Software Bill of Materials (SBOM):

from suppliers, for components that you integrate to software you sell?



2% - We do not sell software
1% N/A / Don't now

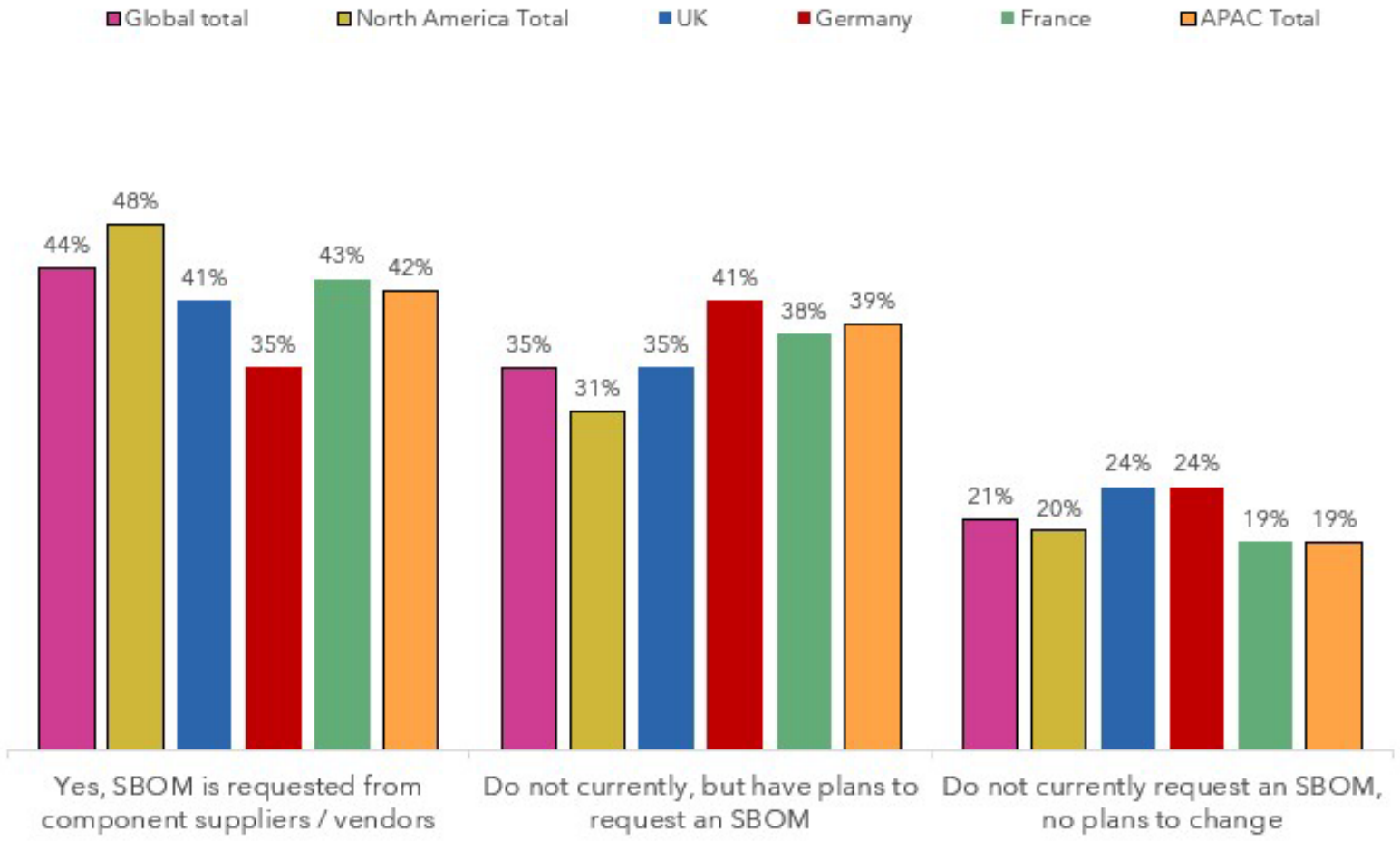
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q16i. Does your organization currently request a Software Bill of Materials (SBOM) from suppliers, for components that you integrate to software you sell?

Requests for a Software Bill of Materials (SBOM):

from vendors that you purchase software from, for use within your organization?



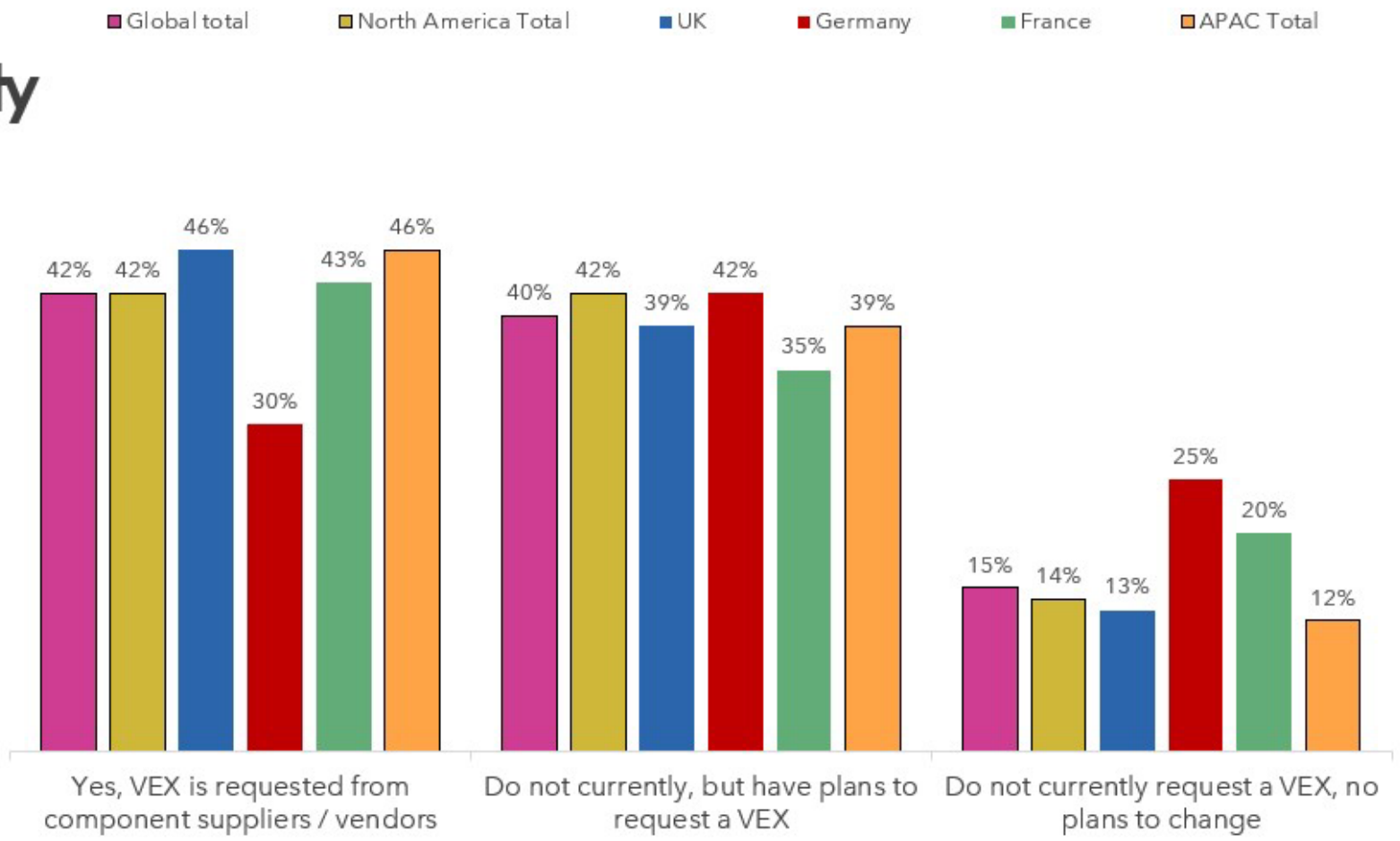
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q16ii. Does your organization currently request a Software Bill of Materials (SBOM) from vendors that you purchase software from, for use within your organization?

Requests for a Vulnerability Exploitability eXchange (VEX) artifact:

from suppliers, for components that you integrate to software you sell?



2% - We do not sell software
1% N/A / Don't now

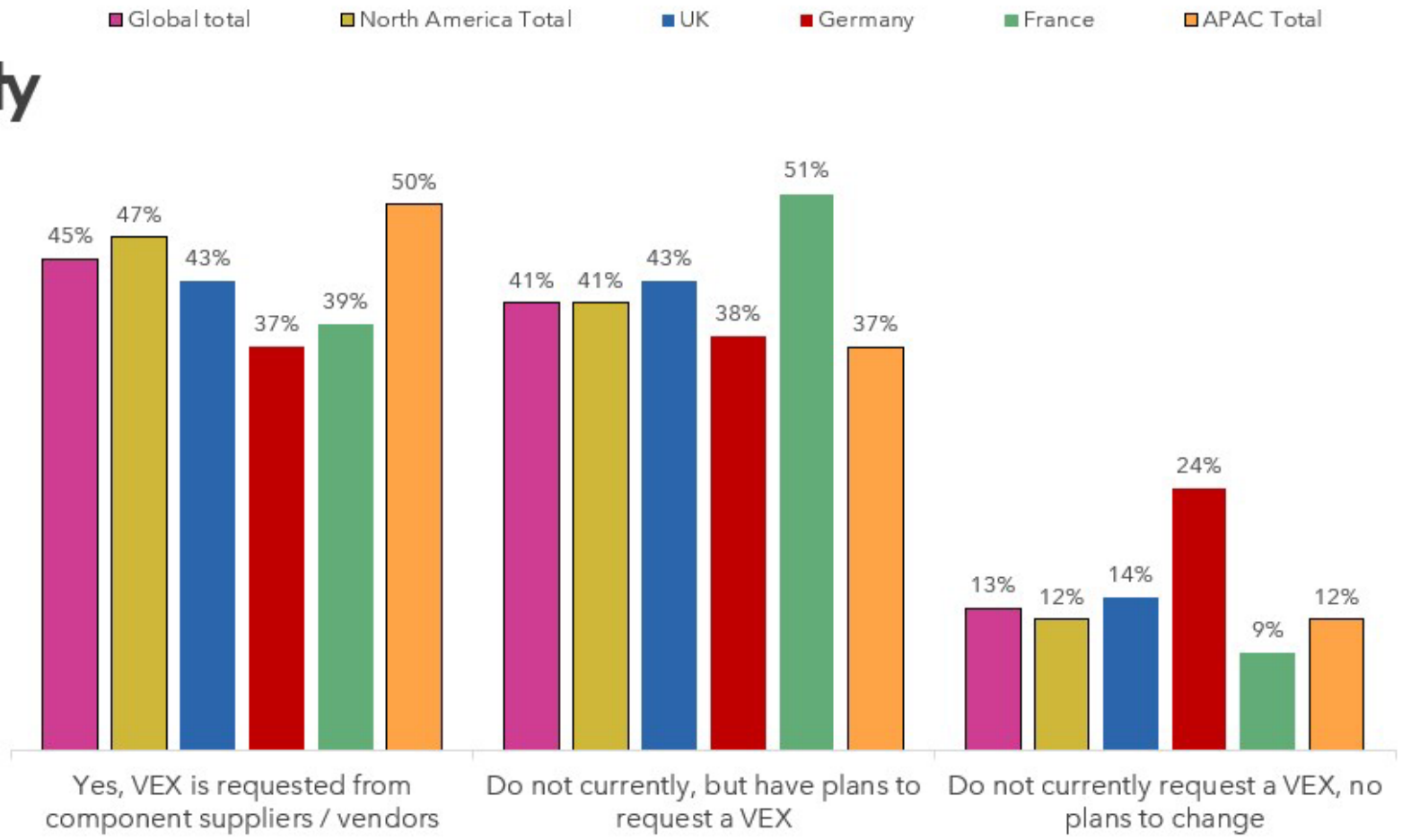
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q17i. Does your organization currently request a Vulnerability Exploitability eXchange (VEX) artifact from suppliers, for components that you integrate to software you sell?

Requests for a Vulnerability Exploitability eXchange (VEX) artifact:

from vendors that you purchase software from, for use within your organization?



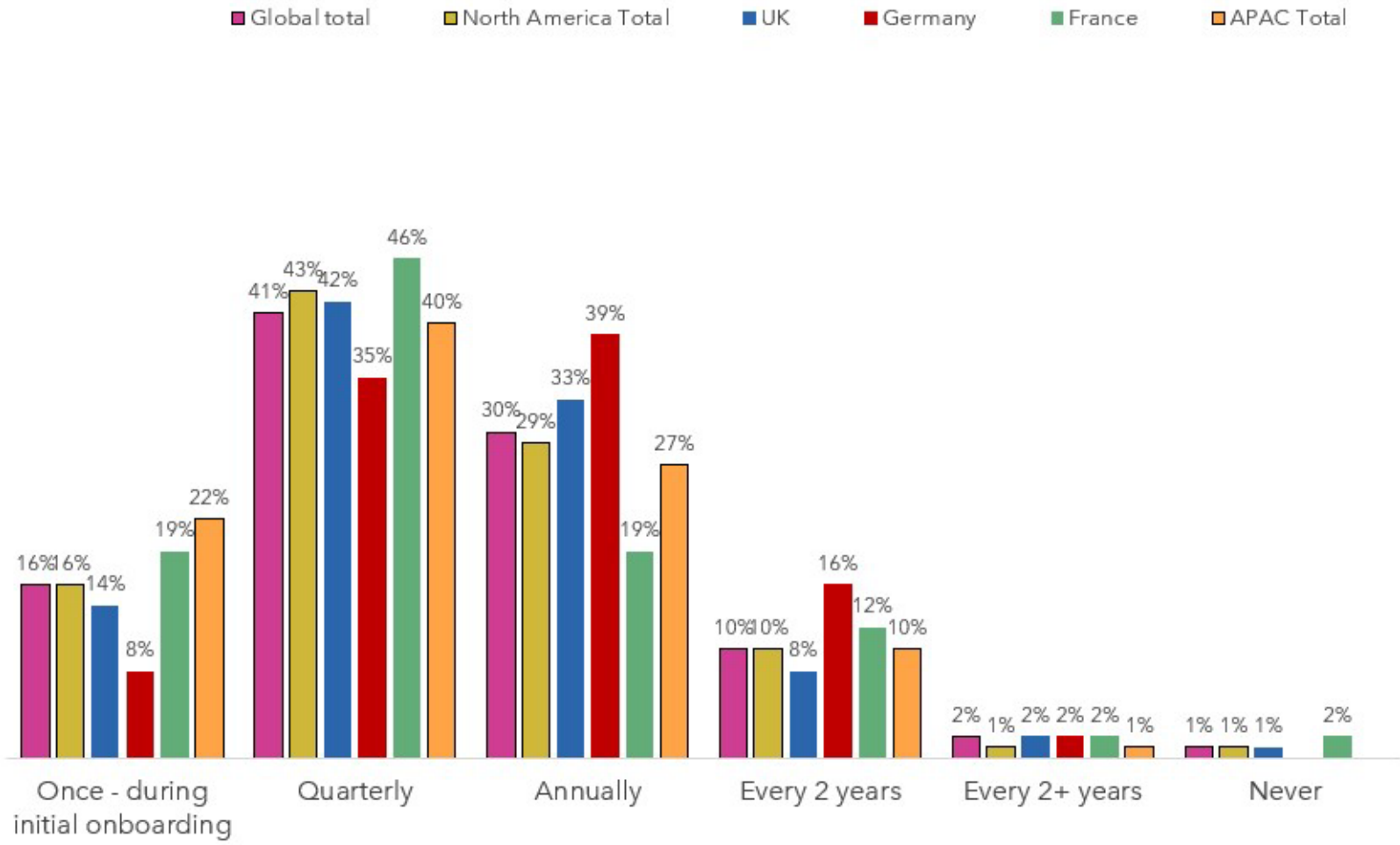
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

1% N/A / Don't now

Single coded question

Q17ii. Does your organization currently request a Vulnerability Exploitability eXchange (VEX) artifact from vendors that you purchase software from, for use within your organization?

Frequency of suppliers/ partners to provide evidence of compliance to security certifications and frameworks



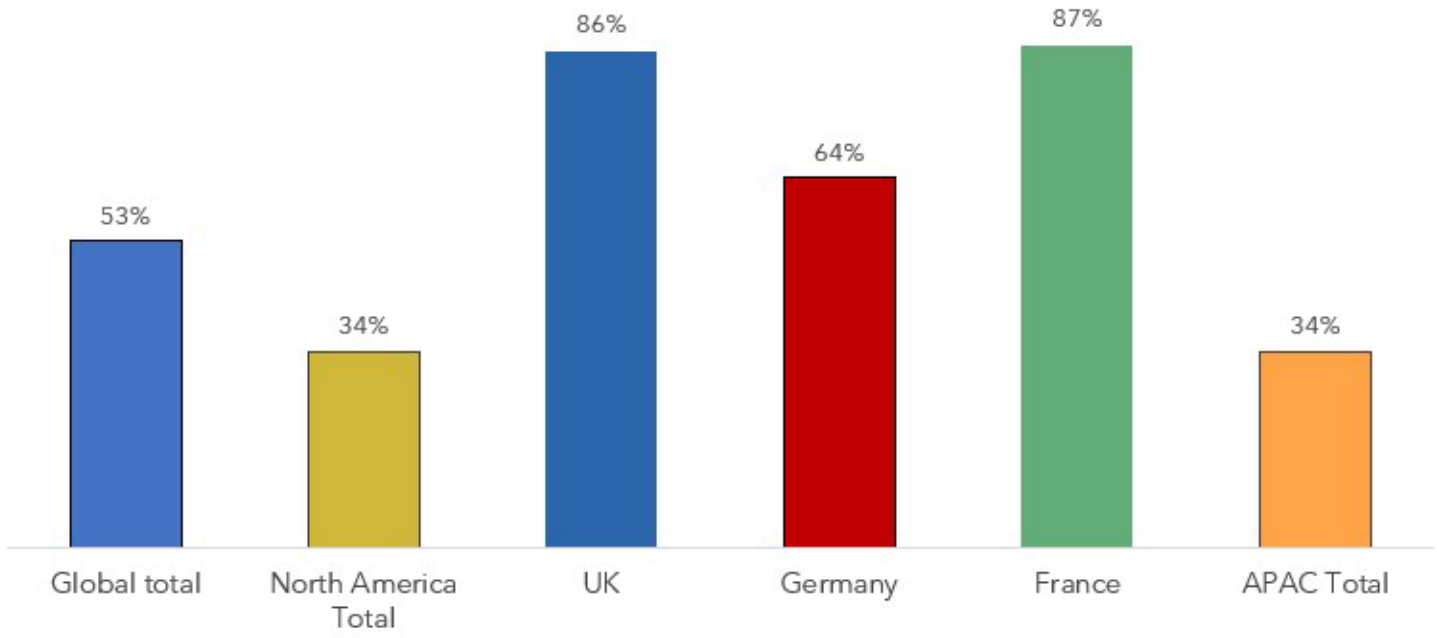
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q17b. Do you require your suppliers/ partners provide evidence of compliance to security certifications and frameworks in your countries of operation?

Requirement to adhere to the Network Information Systems Directive (NIS2)

Yes responses

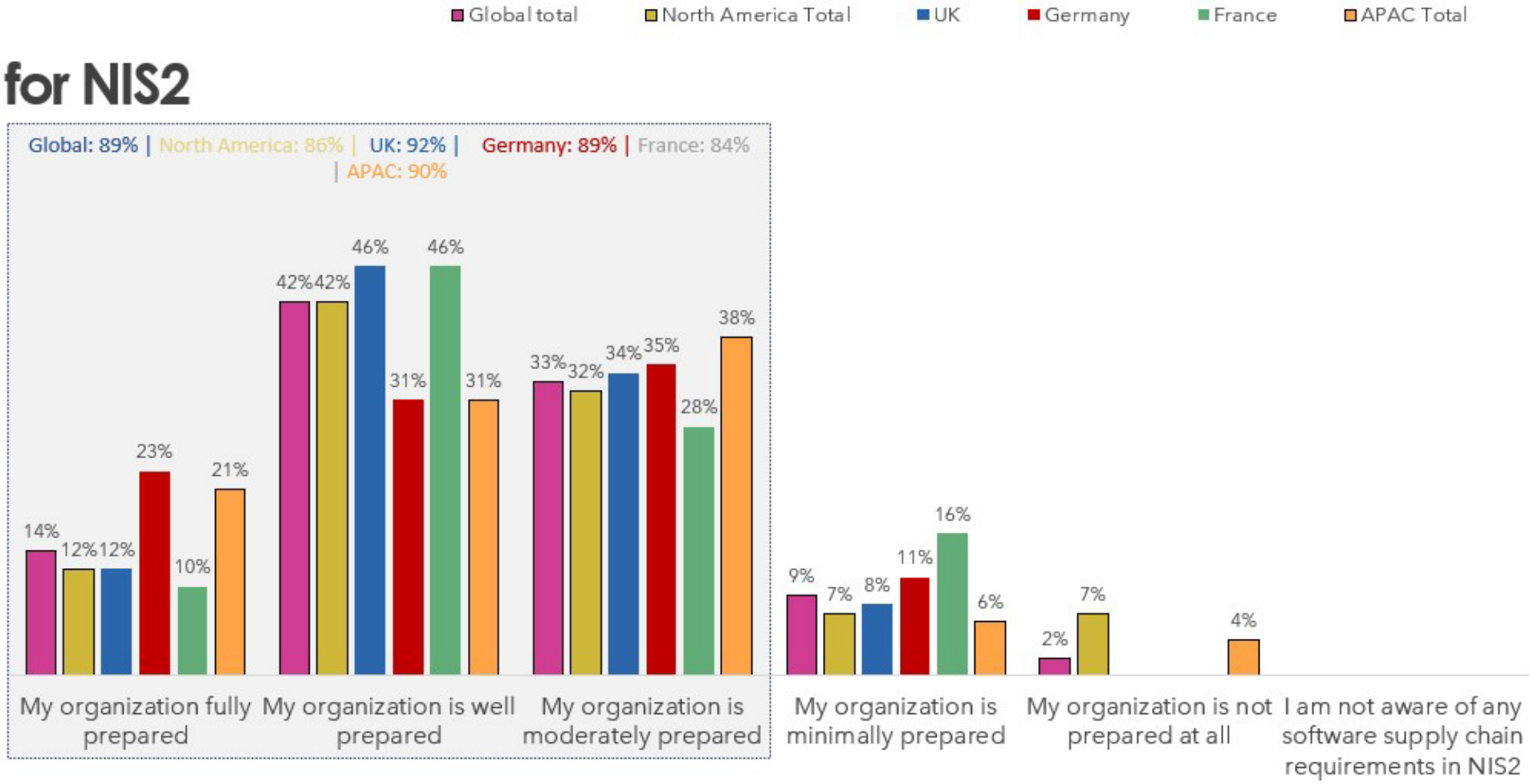


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q18. Is your organization required to adhere to the Network Information Systems Directive (NIS2)?

Preparedness for NIS2 compliance relating to security of software supply chains

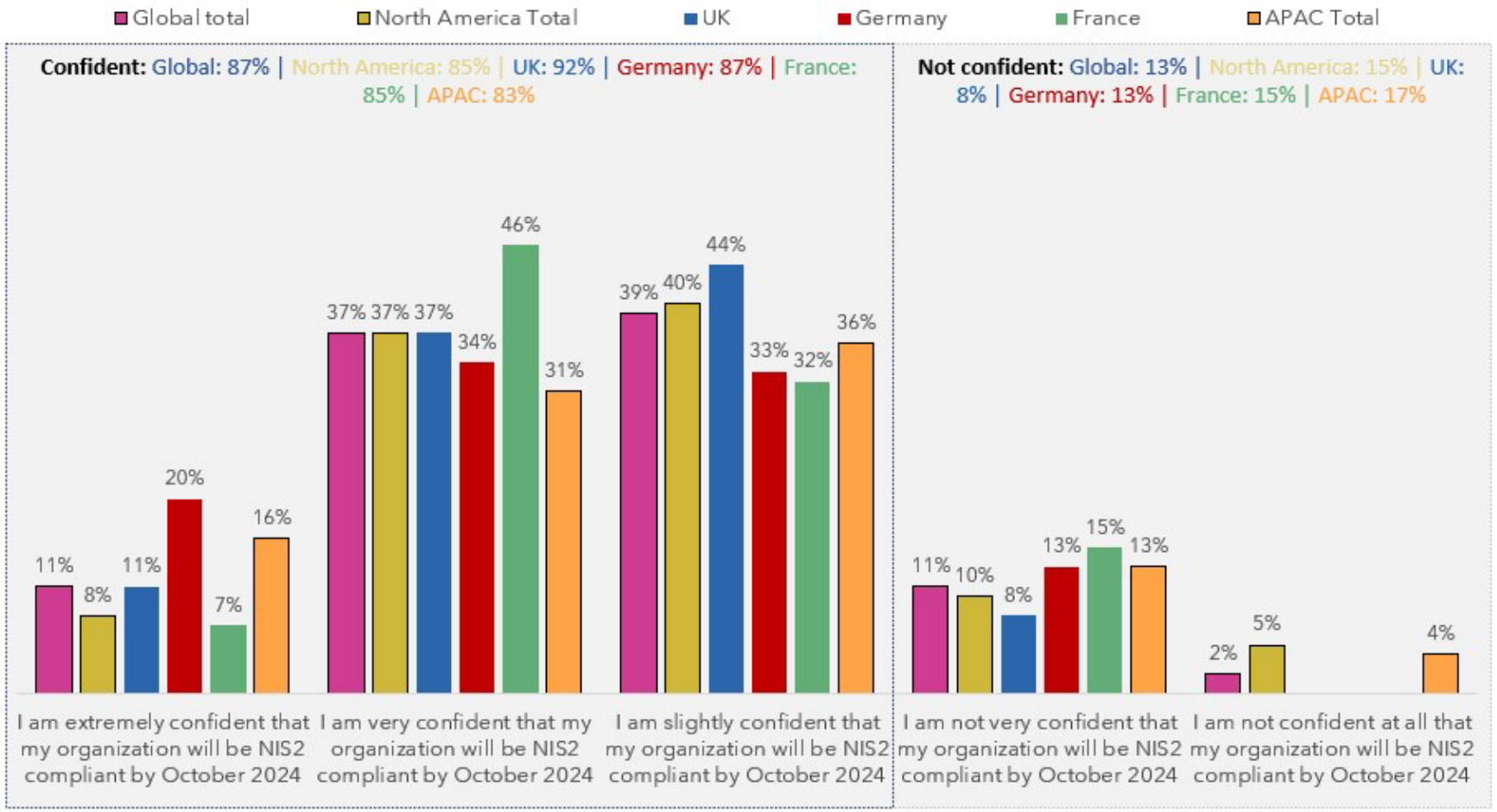


Base: Organizations that are required to adhere to the NIS2 Directive (525) North America (135) UK (171) Germany (64) France (87) APAC total (68)

Single coded question

Q18b. How prepared is your organization today for compliance with the NIS2 requirements relating to security of software supply chains?

Confidence that organization will be NIS2 compliant by October 2024 deadline

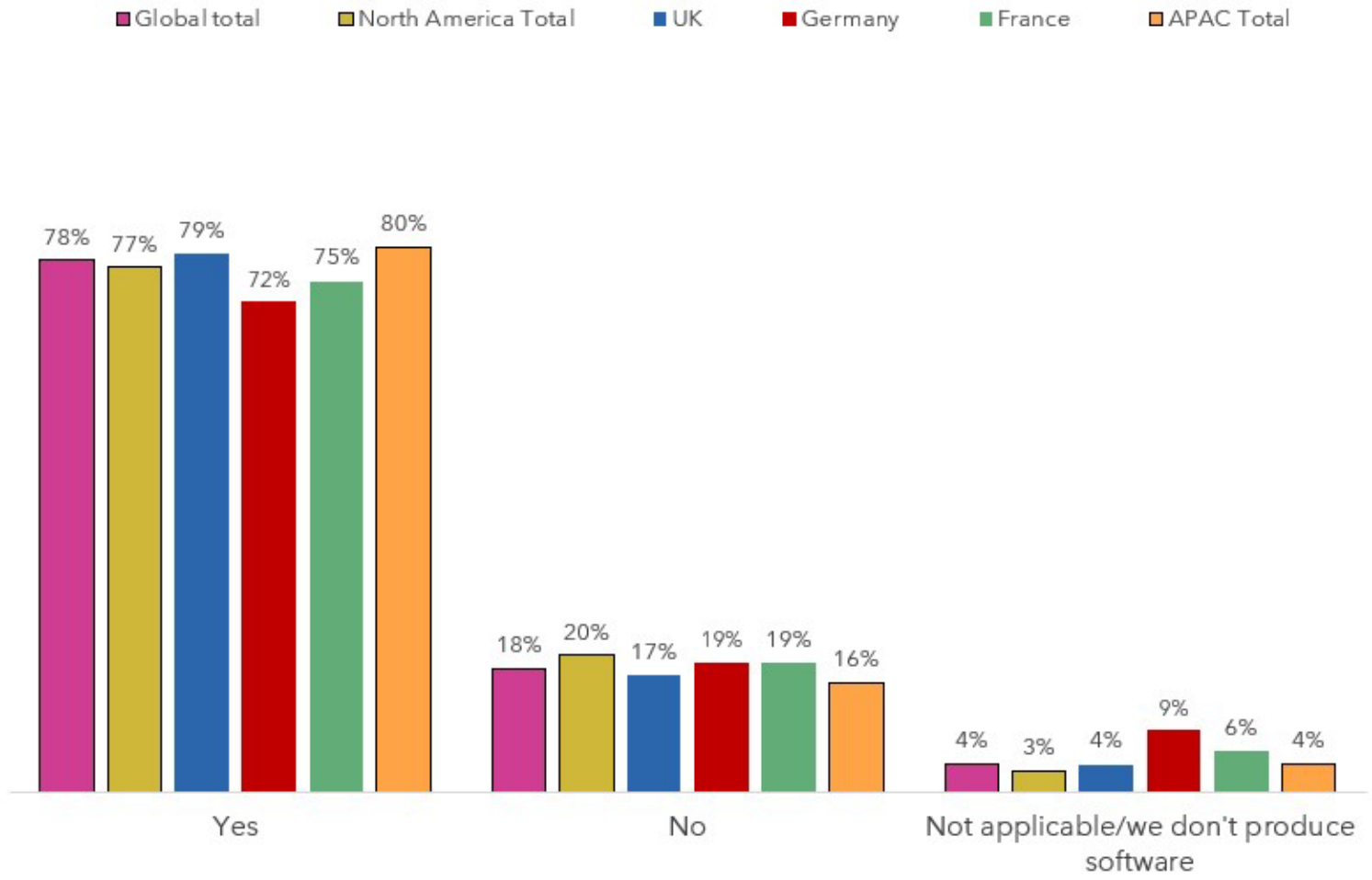


Base: Organizations that are required to adhere to the NIS2 Directive (525) North America (135) UK (171) Germany (64) France (87) APAC total (68)

Single coded question

Q18c. How confident are you that your organization will be NIS2 compliant in time for the October 2024 deadline?

Tracking the impact of vulnerabilities within supply chain of software produced to downstream consumers

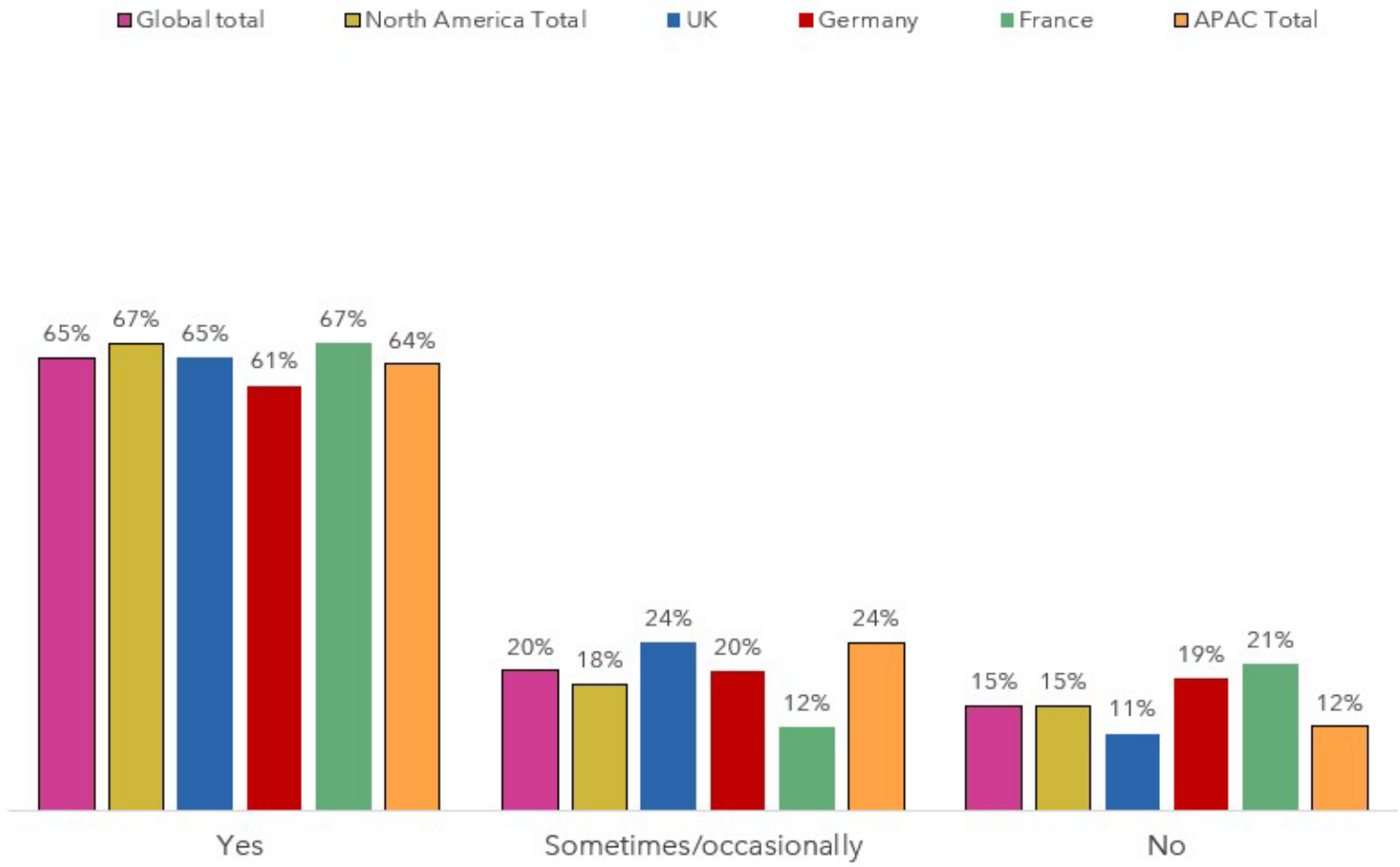


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

Q19. Do you track the impact of vulnerabilities within the supply chain of software you produce, to your downstream consumers?

Communicating vulnerabilities discovered in software produced to downstream consumers

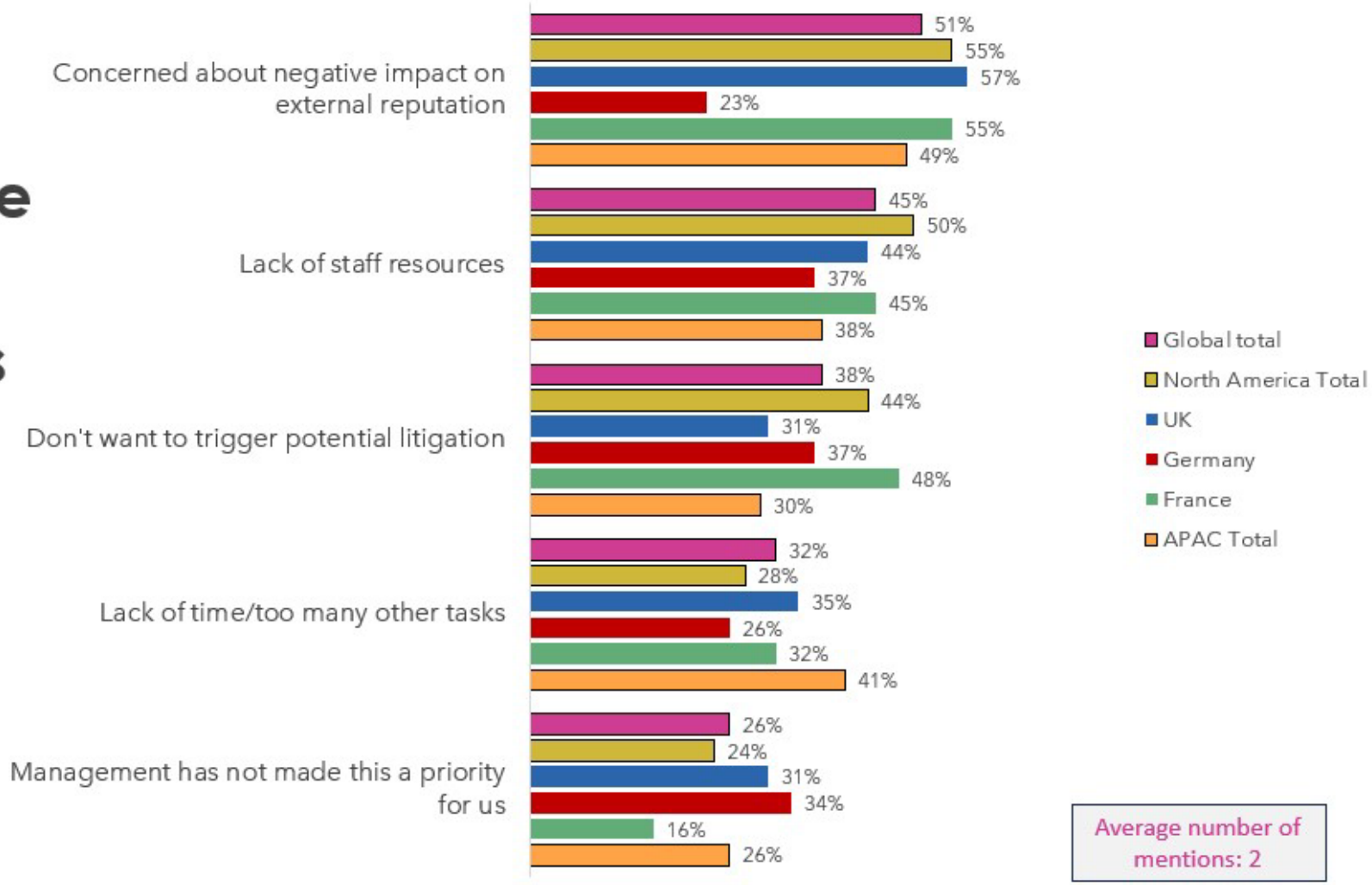


Base: All except those who don't produce software (959) North America (389) UK (192) Germany (91) France (94) APAC total (193)

Single coded question

Q20. Do you communicate the vulnerabilities you discover in the software you produce to downstream consumers?

Biggest obstacles to communicating software vulnerabilities to downstream consumers



Average number of mentions: 2

Base: Organisations where vulnerabilities are not communicated frequently (334) North America (131) UK (68) Germany (35) France (31) APAC total (69)

Multi coded question

Q20b. What are the biggest obstacles to communicating software vulnerabilities to downstream consumers?

Appendix

2022 vs 2024 Comparison Charts

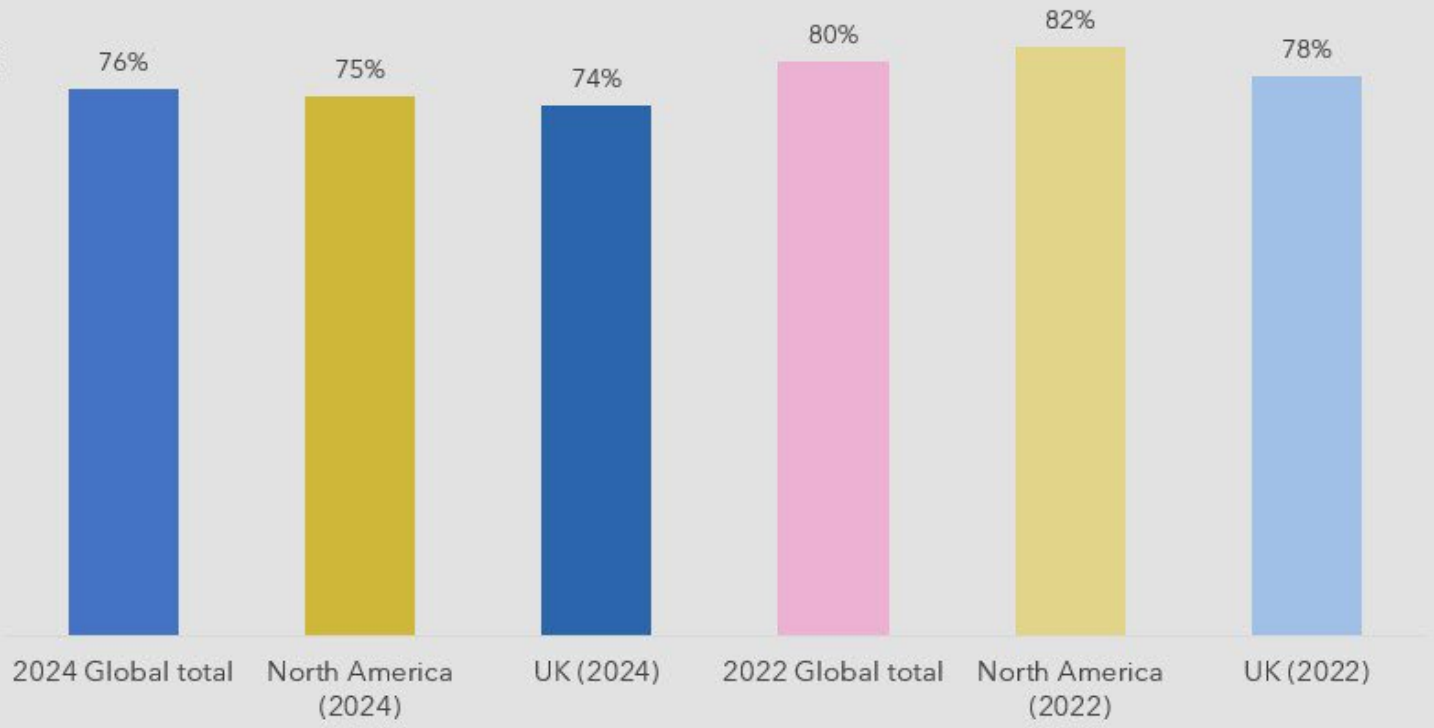
BlackBerry Intelligent Security. Everywhere.

Coleman Parkes

2024 vs 2022 comparison

Yes responses

Being notified of a vulnerability or attack within software supply chain in last 12 months



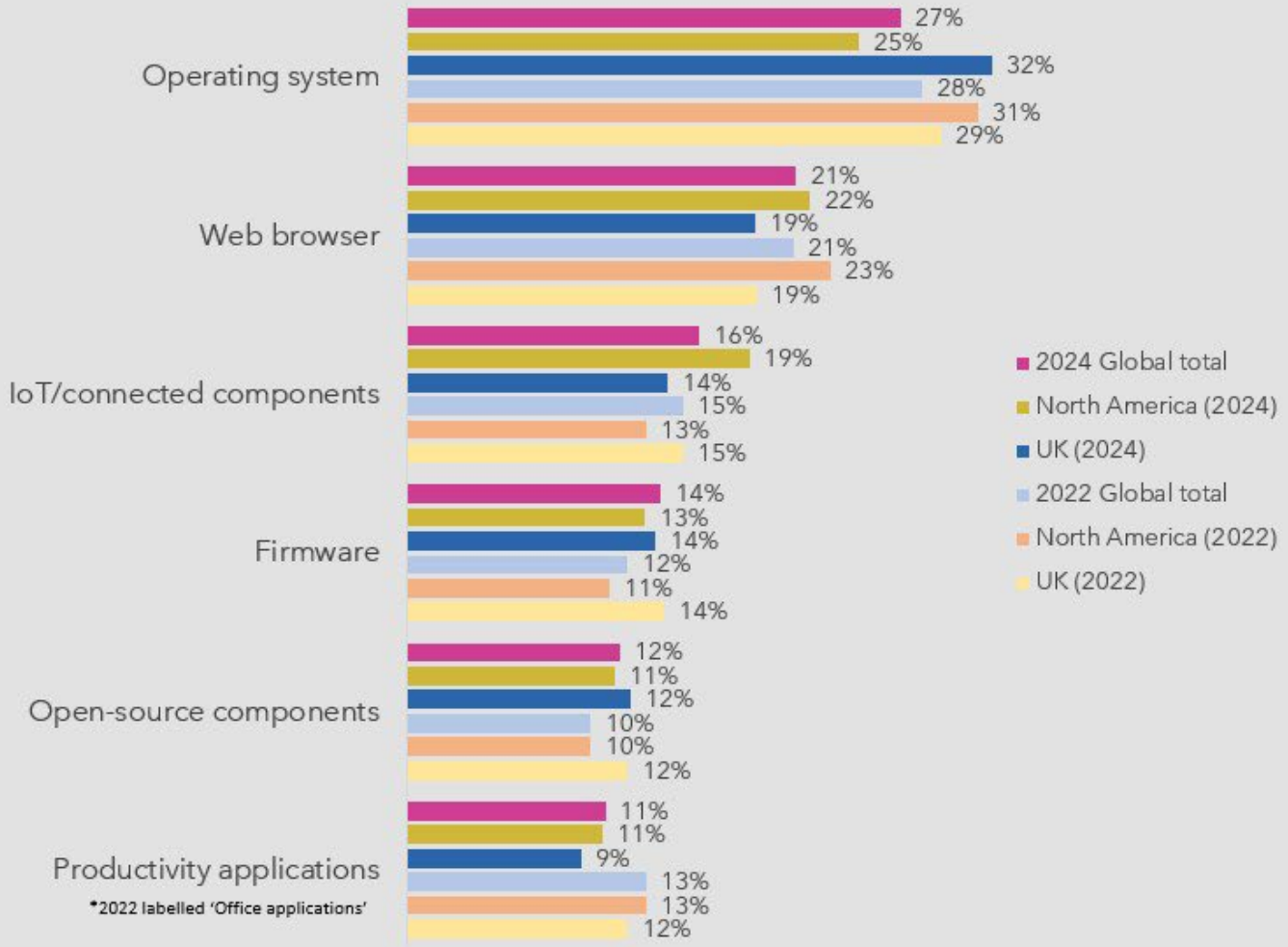
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q1. Has your organization been notified of a vulnerability or attack within the supply chain of software you consume in the last 12 months?

2024 vs 2022 comparison

Vulnerable components having the biggest impact for organization



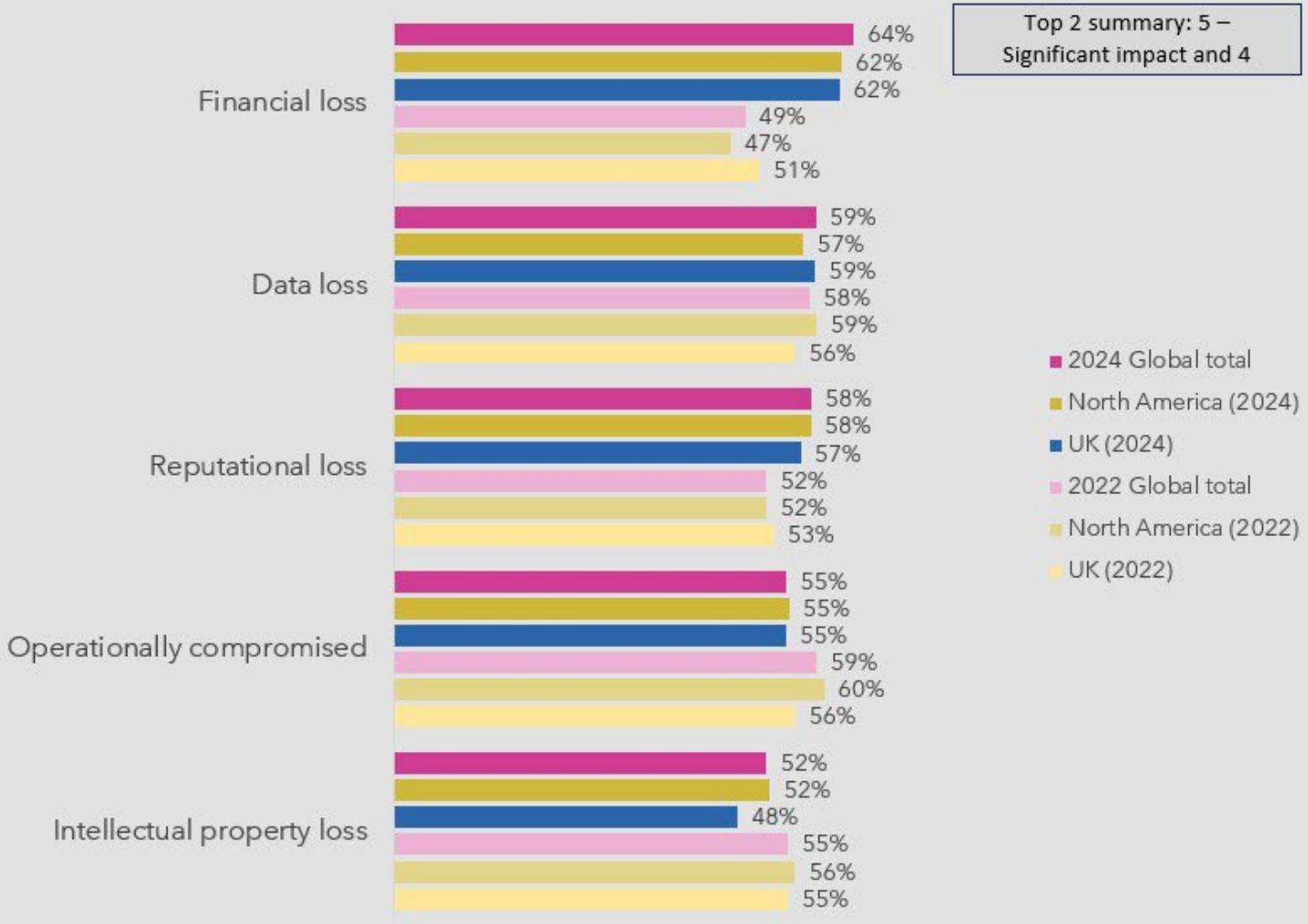
Base: Respondents who have been notified of a vulnerability or attack within their supply chain <2024> (761) North America (301) UK (148) <2022> (1,202) North America (410) UK (391)

Single coded question

Q2. Which of the following vulnerable components, resulted in the biggest impact for your organization?

2024 vs 2022 comparison

Significance of the attack on the business



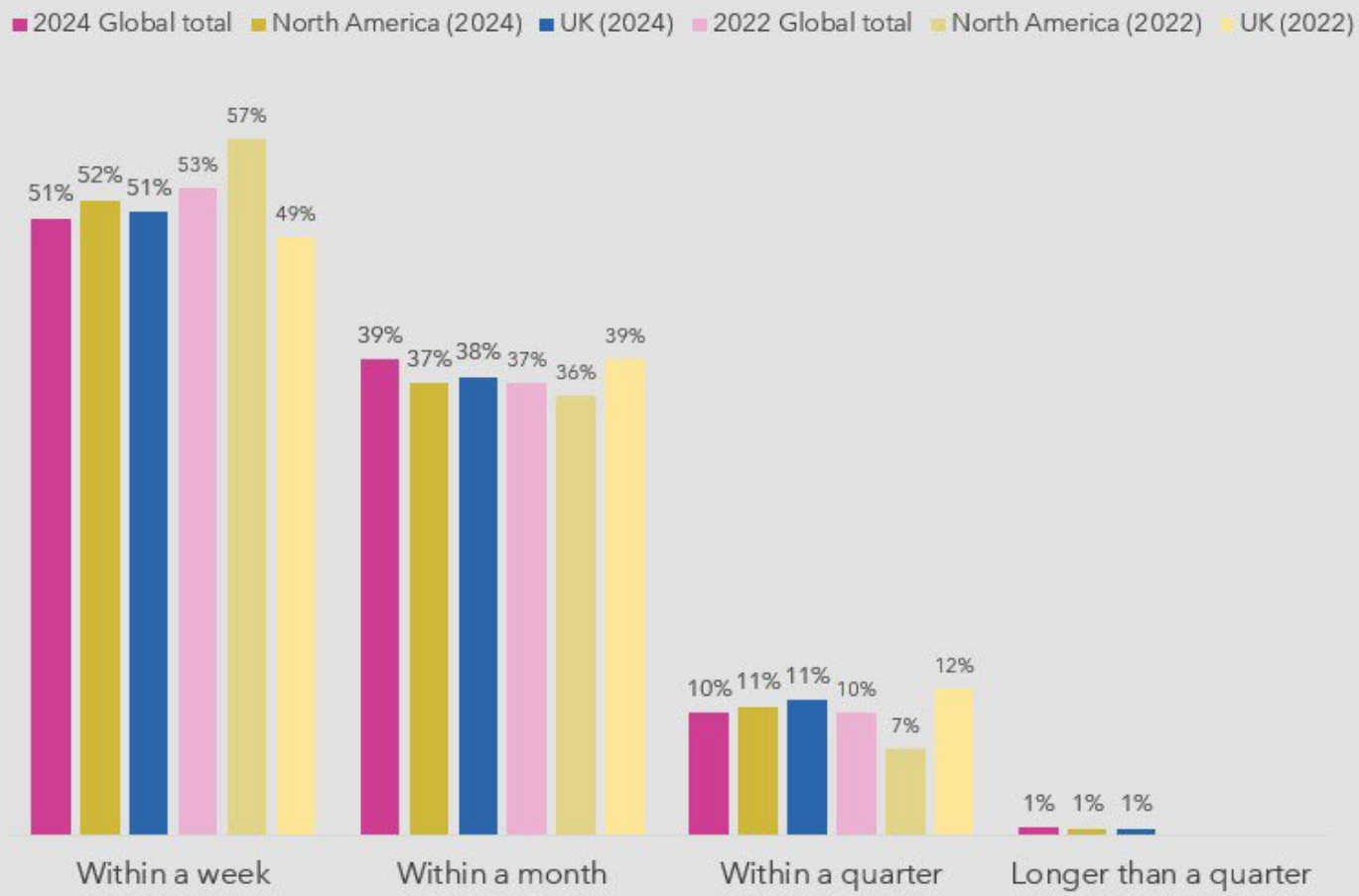
Base: Respondents who have been notified of a vulnerability or attack within their supply chain <2024> (761) North America (301) UK (148) <2022> (1,202) North America (410) UK (391)

Single code per option

Q3. How significant was the impact of the attack on each of the below?

2024 vs 2022 comparison

Time taken to fully recover from an exploited vulnerability in software supply chain



Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

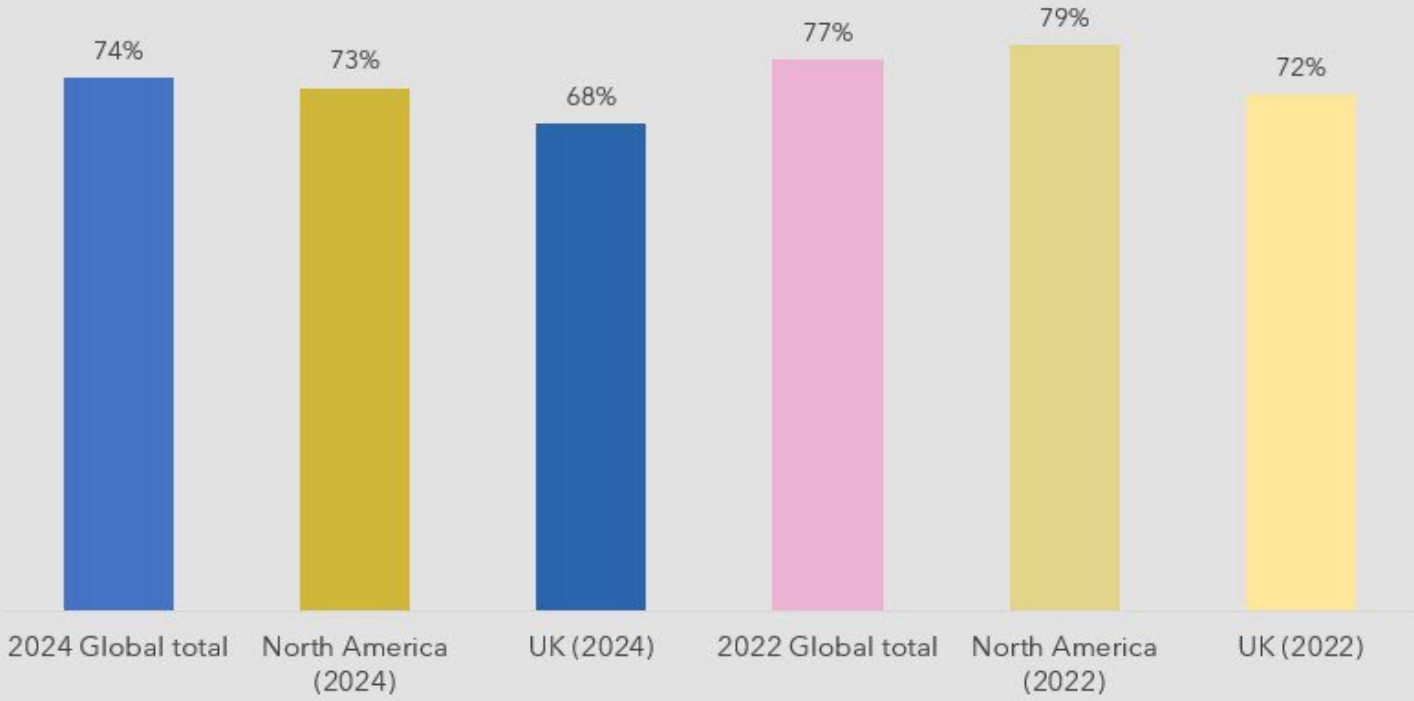
Single coded question

Q4. On average, how long does it take to fully recover from an exploited vulnerability in your software supply chain?

2024 vs 2022 comparison

Made aware of a member of supply chain not previously aware of / monitoring for security practices

Yes responses



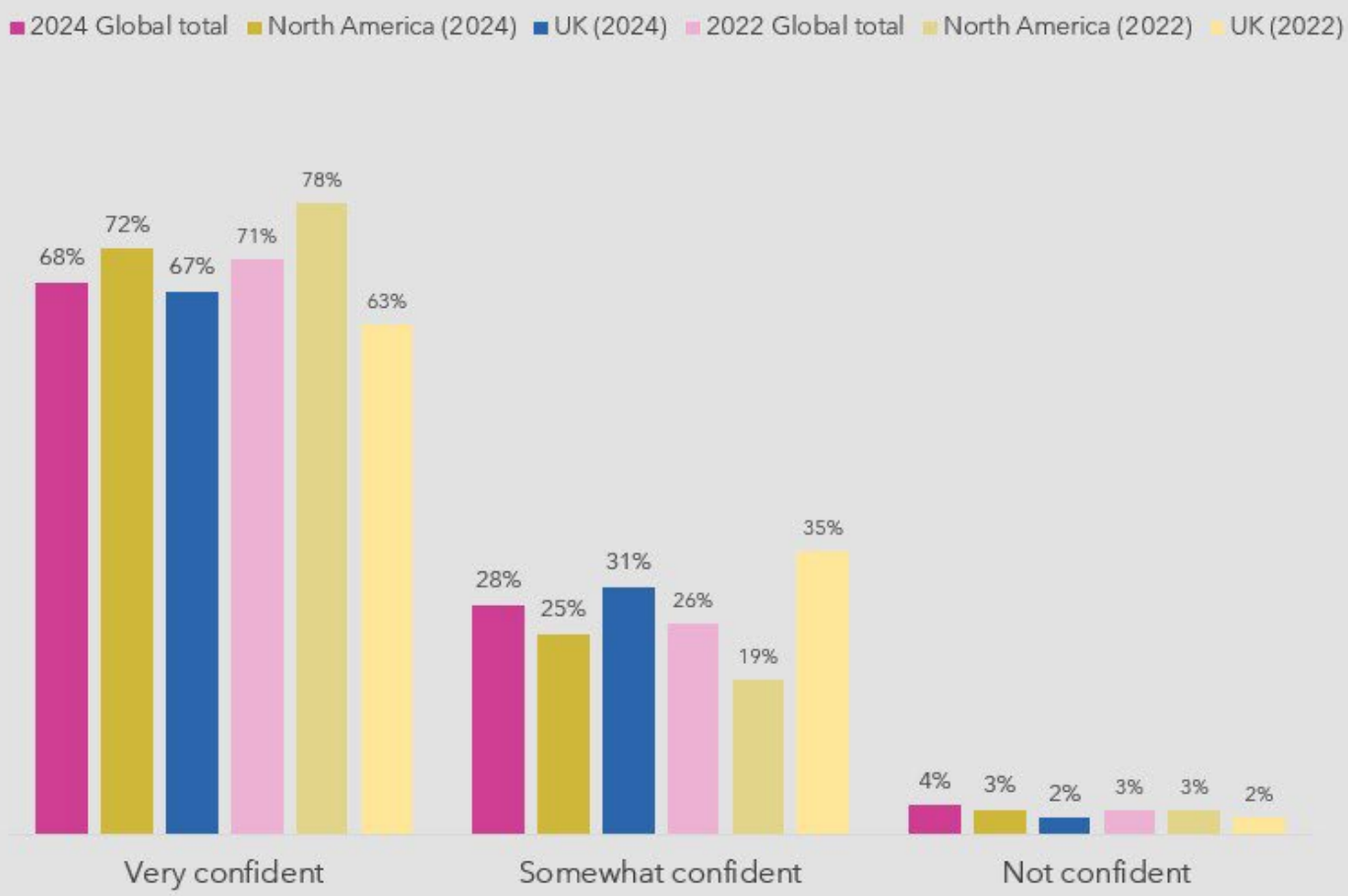
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q5. Over the last year, have you been made aware of a member of your supply chain that you weren't previously aware of / monitoring for security practices?

2024 vs 2022 comparison

Confidence that suppliers / partners can identify and prevent a vulnerability



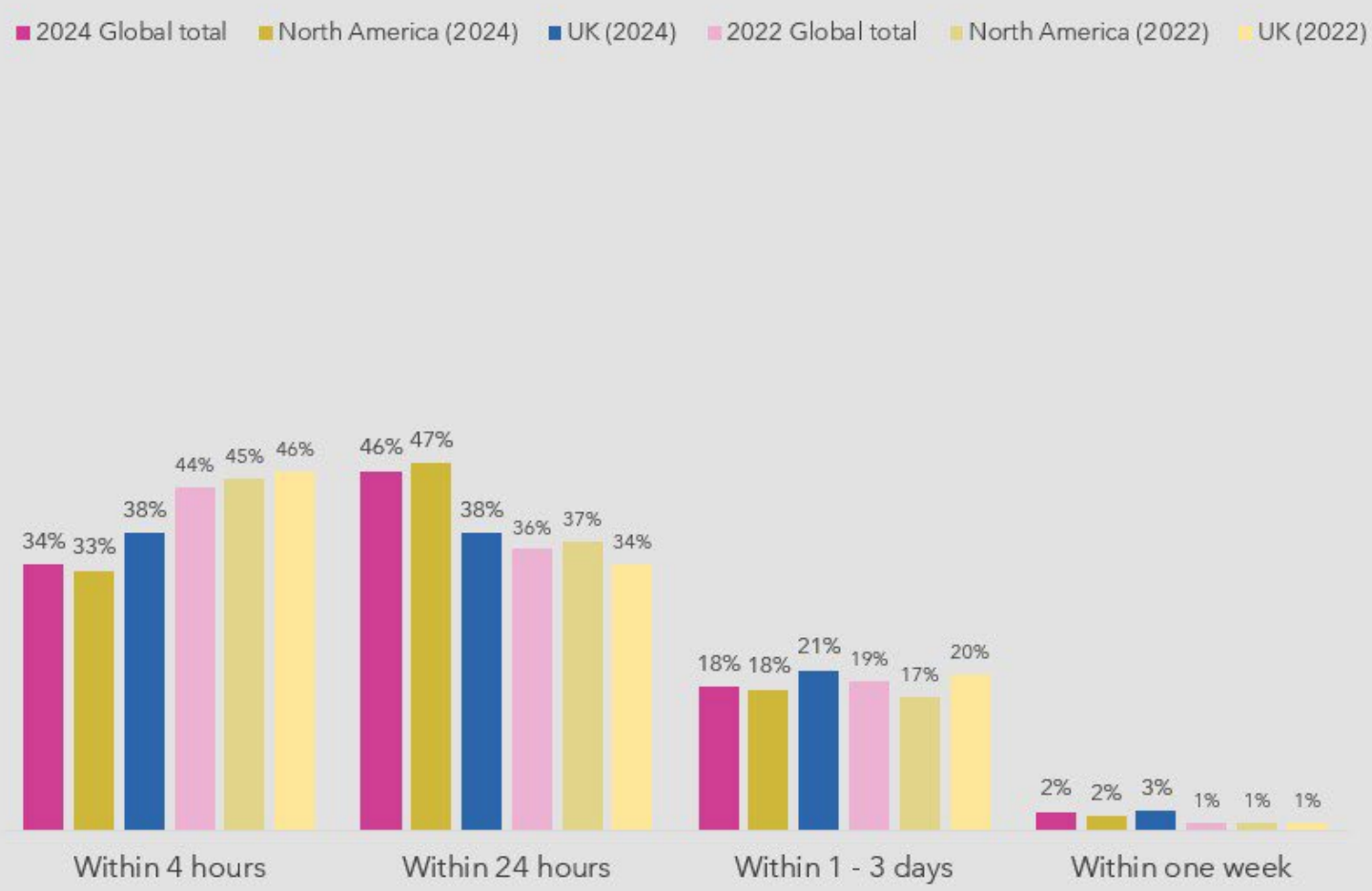
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q7. How confident are you that your suppliers / partners can identify and prevent exploit of a vulnerability within their environment?

2024 vs 2022 comparison

Expected time taken to be notified in the event of a supplier / partner suffering a cyber breach



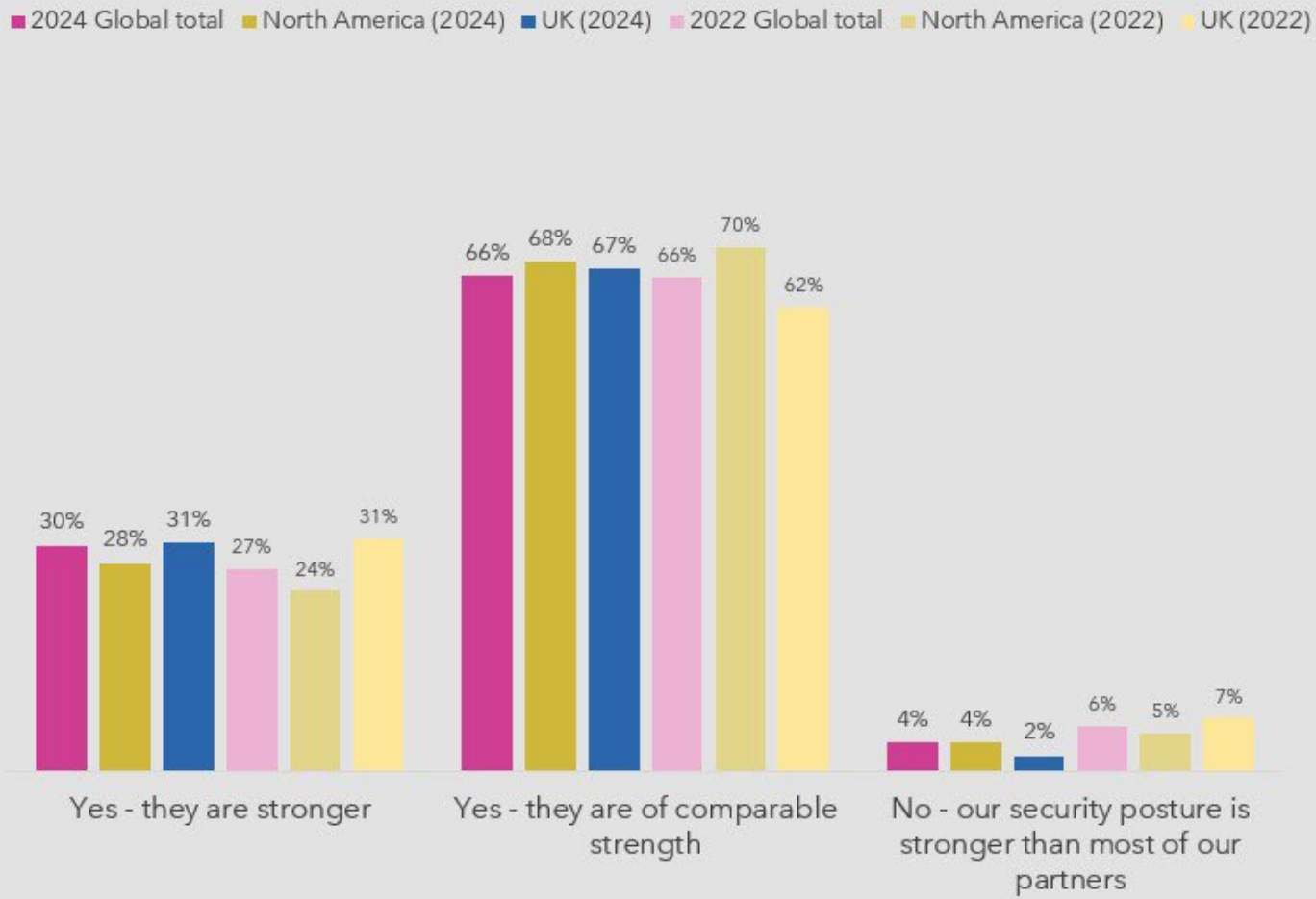
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q8. How quickly do you expect to be notified in the event of a supplier / partner within your software supply chain suffering a cyber breach?

2024 vs 2022 comparison

Comparability of suppliers / partners cybersecurity policies



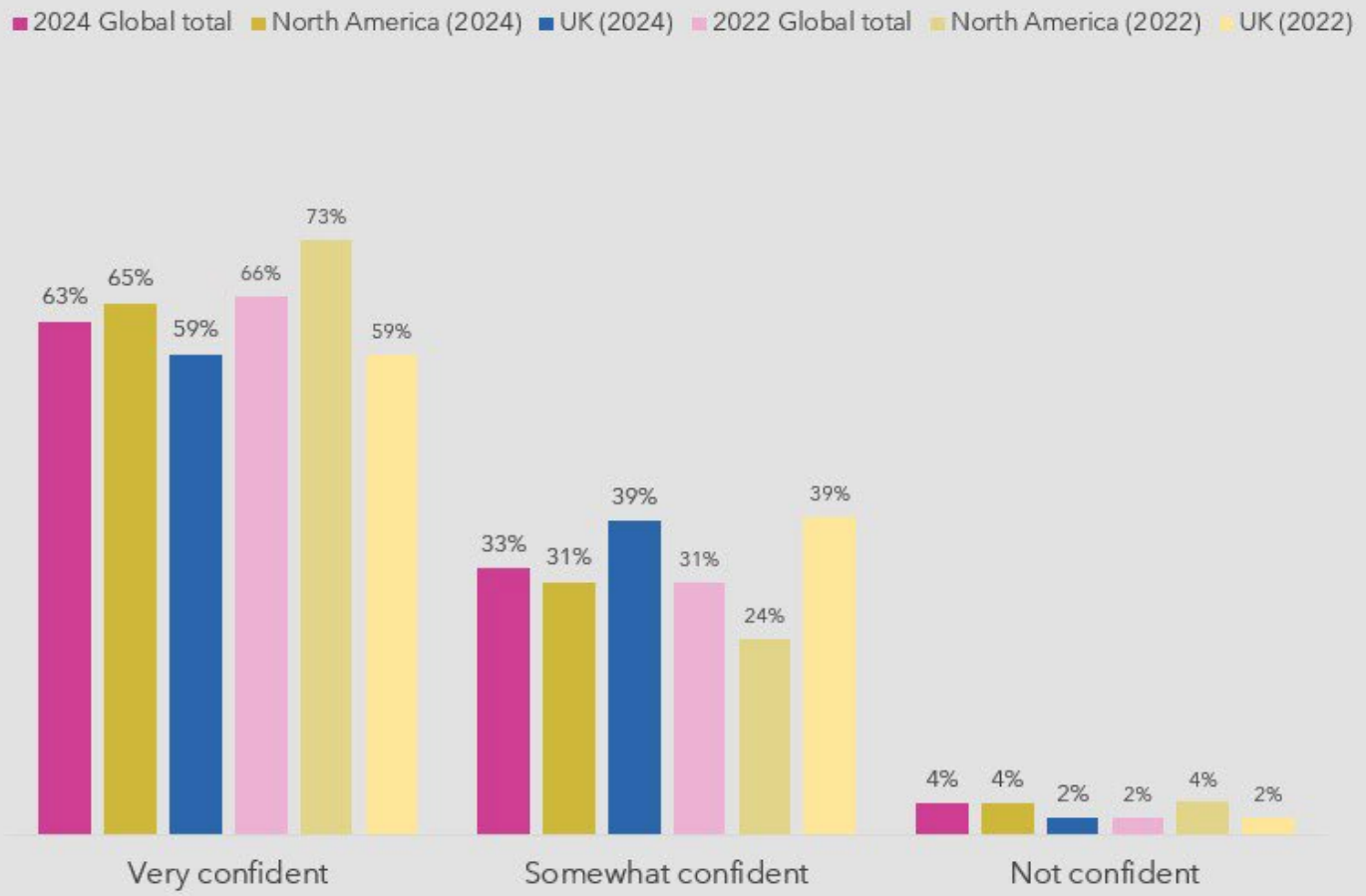
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q9. Do you believe the suppliers / partners of your software supply chain cybersecurity policies are comparable to those implemented at your company?

2024 vs 2022 comparison

Confidence that suppliers / supply chain partners have adequate cybersecurity regulatory and compliance practice



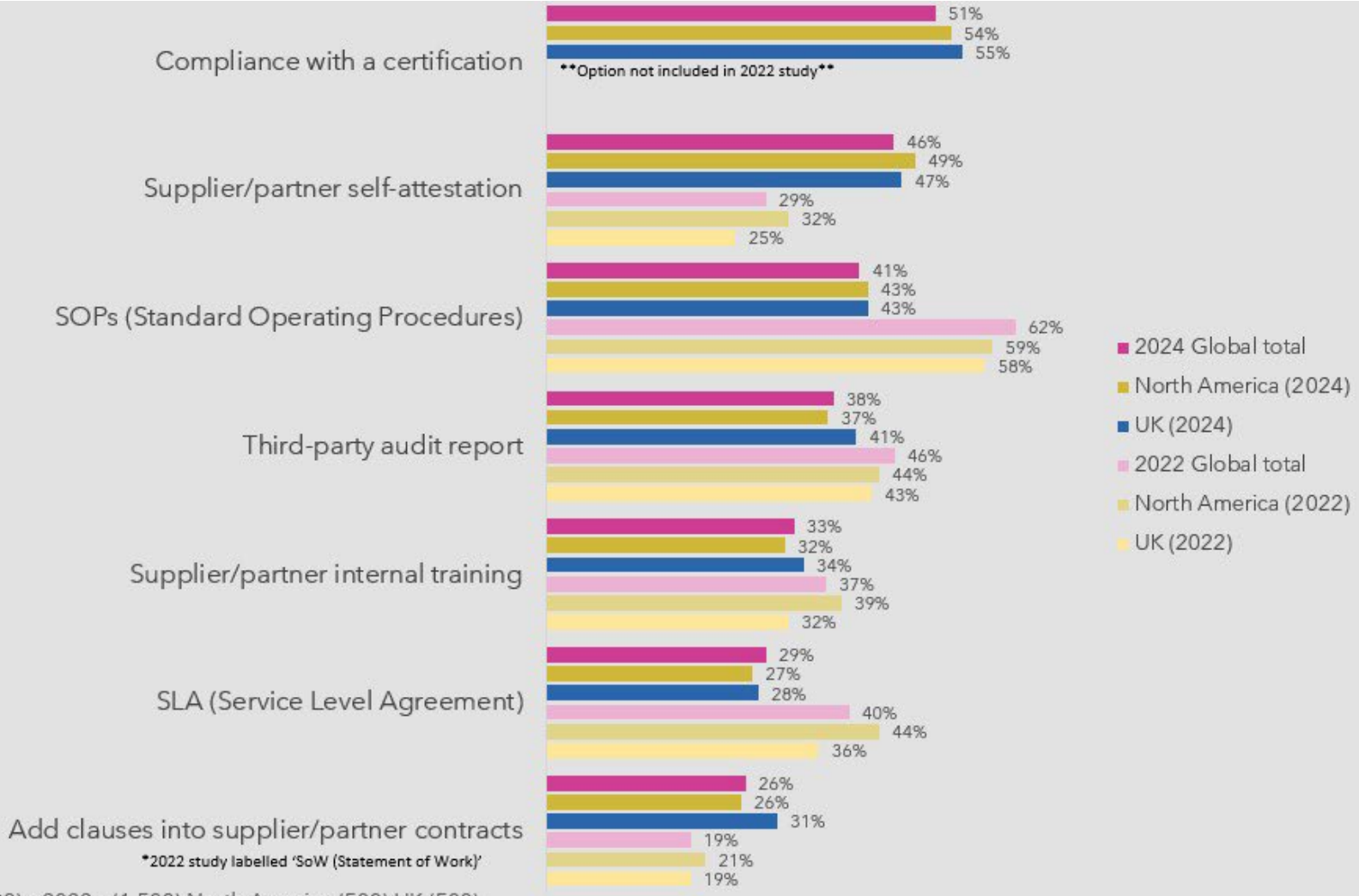
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q10. How confident are you that your suppliers / supply chain partners have adequate cybersecurity regulatory and compliance practice?

2024 vs 2022 comparison

Evidence required for suppliers / partners to attest level of securing software supply chain



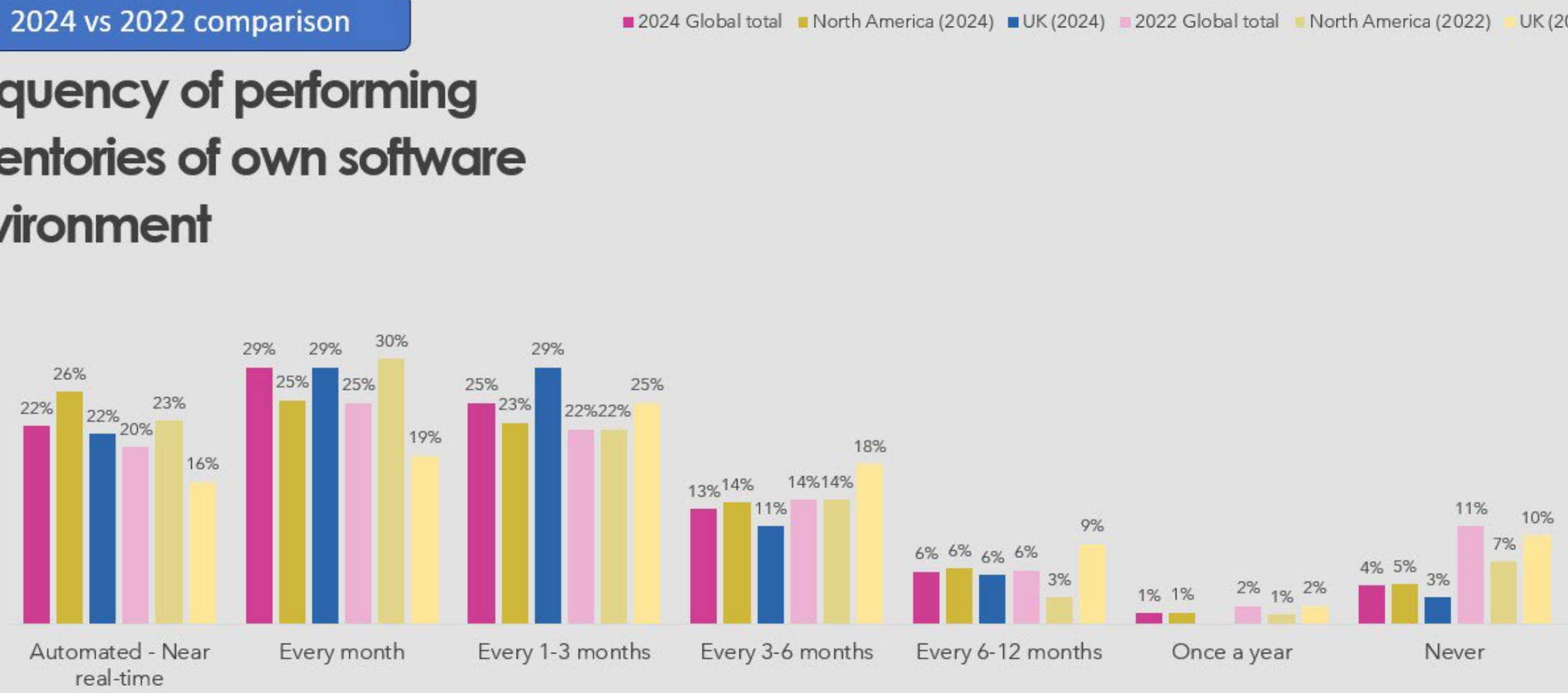
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Multi coded question

Q11. What evidence do you require your suppliers / partners to attest to their level of securing their software supply chain?

2024 vs 2022 comparison

Frequency of performing inventories of own software environment



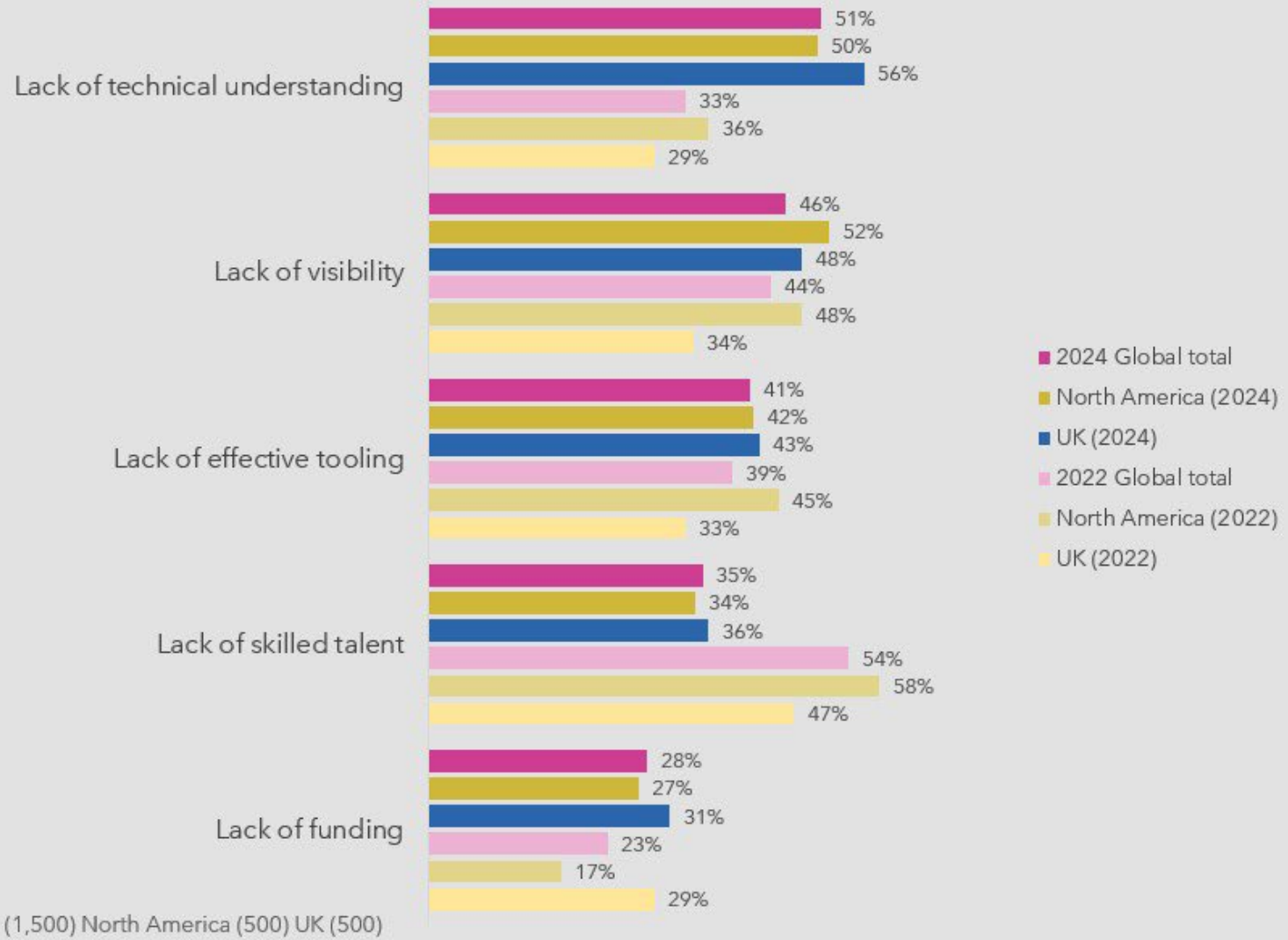
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q12. How often do you perform an inventory of your own software environment?

2024 vs 2022 comparison

Biggest barriers to regular software inventories



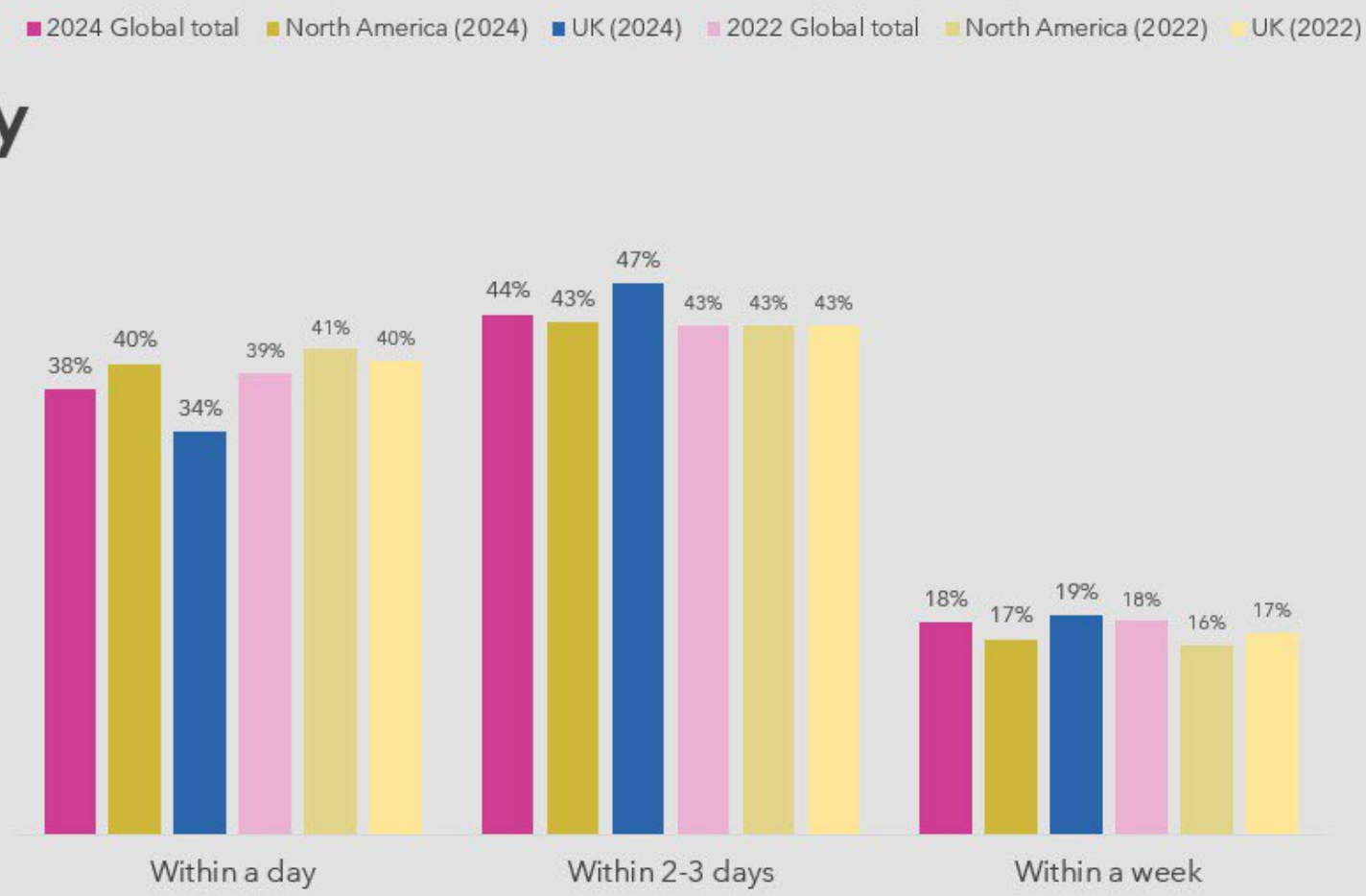
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Multi coded question

Q13. What are the biggest barriers to regular software inventories?

2024 vs 2022 comparison

Average time taken to identify if an impacted library is used following a vulnerability



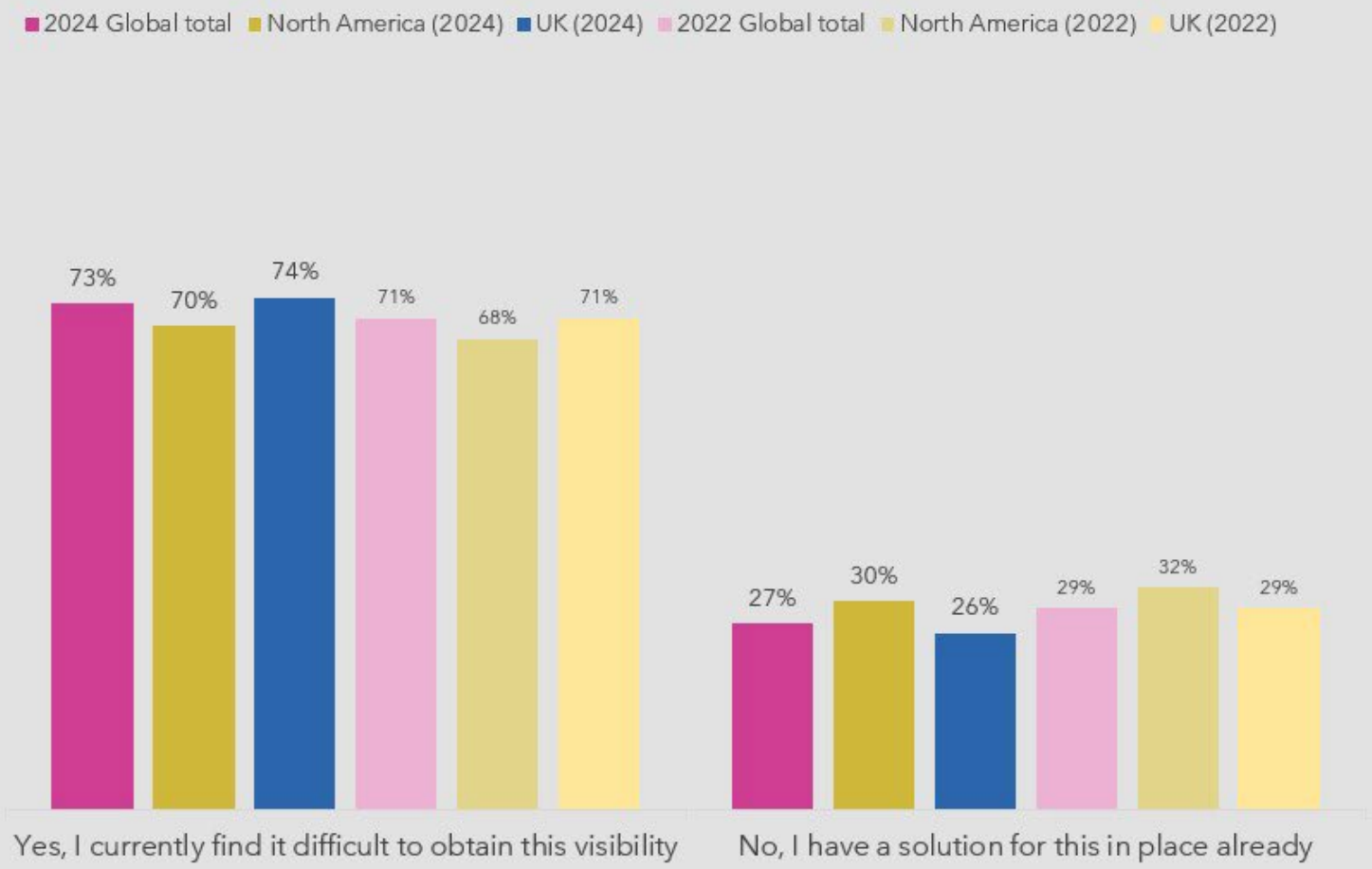
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q14. You have become aware of a vulnerability that may impact the supply chain of software you consume. From the time you start your investigation, on average, how long does it take your organization to identify if an impacted library is used in any of the software you consume?

2024 vs 2022 comparison

Usefulness of tool to inventory software libraries and bring greater visibility to software impacted by a vulnerability



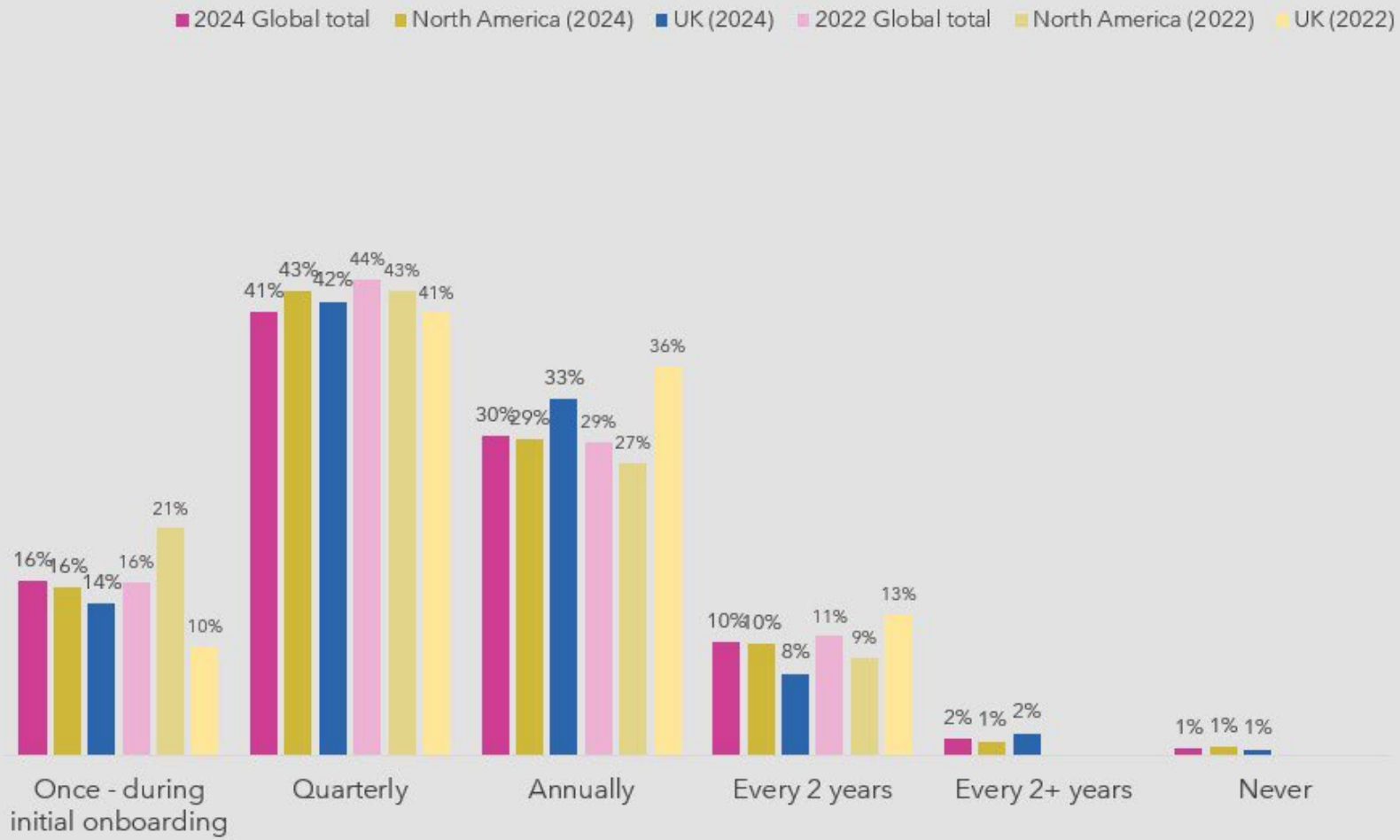
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q15. Would you find a tool that could inventory software libraries within your supply chain and bring greater visibility to software impacted by a vulnerability useful?

2024 vs 2022 comparison

Frequency of suppliers/ partners to provide evidence of compliance to security certifications and frameworks



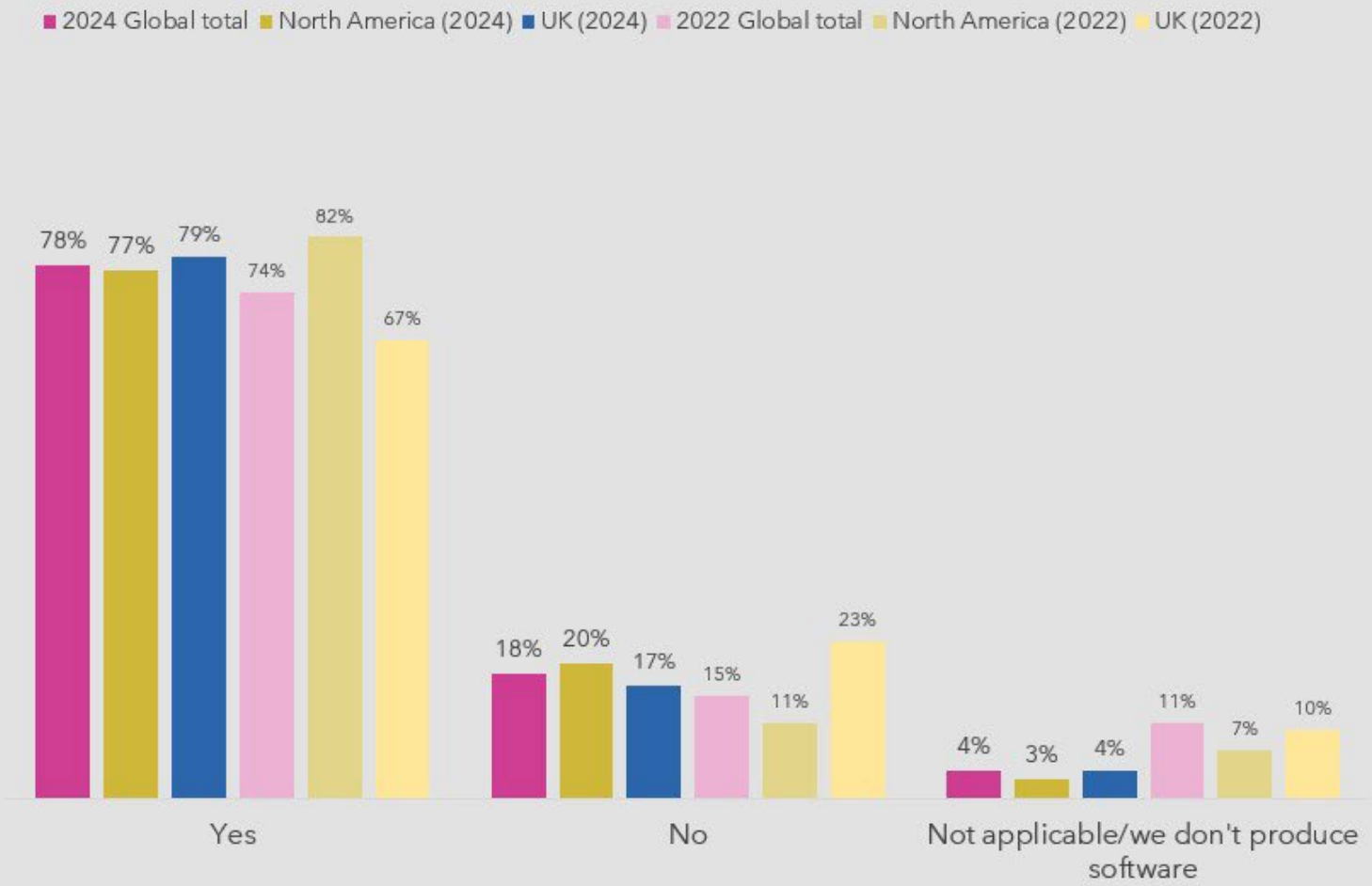
Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q17b. Do you require your suppliers/ partners provide evidence of compliance to security certifications and frameworks in your countries of operation?

2024 vs 2022 comparison

Tracking the impact of vulnerabilities within supply chain of software produced to downstream consumers



Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

Single coded question

Q19. Do you track the impact of vulnerabilities within the supply chain of software you produce, to your downstream consumers?

BlackBerry | Cybersecurity

Thank You

Christine Gadsby

Vice President & CISO, Cybersecurity

May 2024

Coleman Parkes