

Software supply chain research

Blackberry

Final Global results presented by Gabrielle Mastin and Ian Beston

May 2024



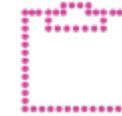
Study Detail



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

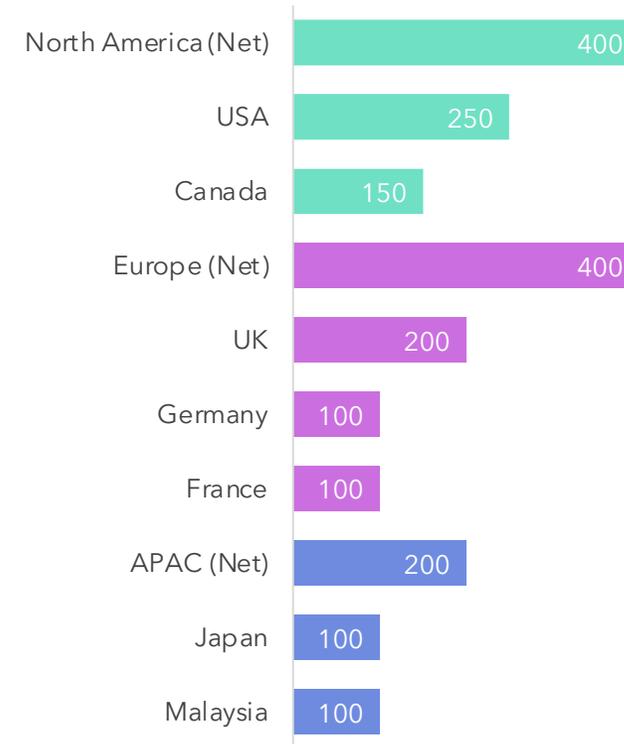
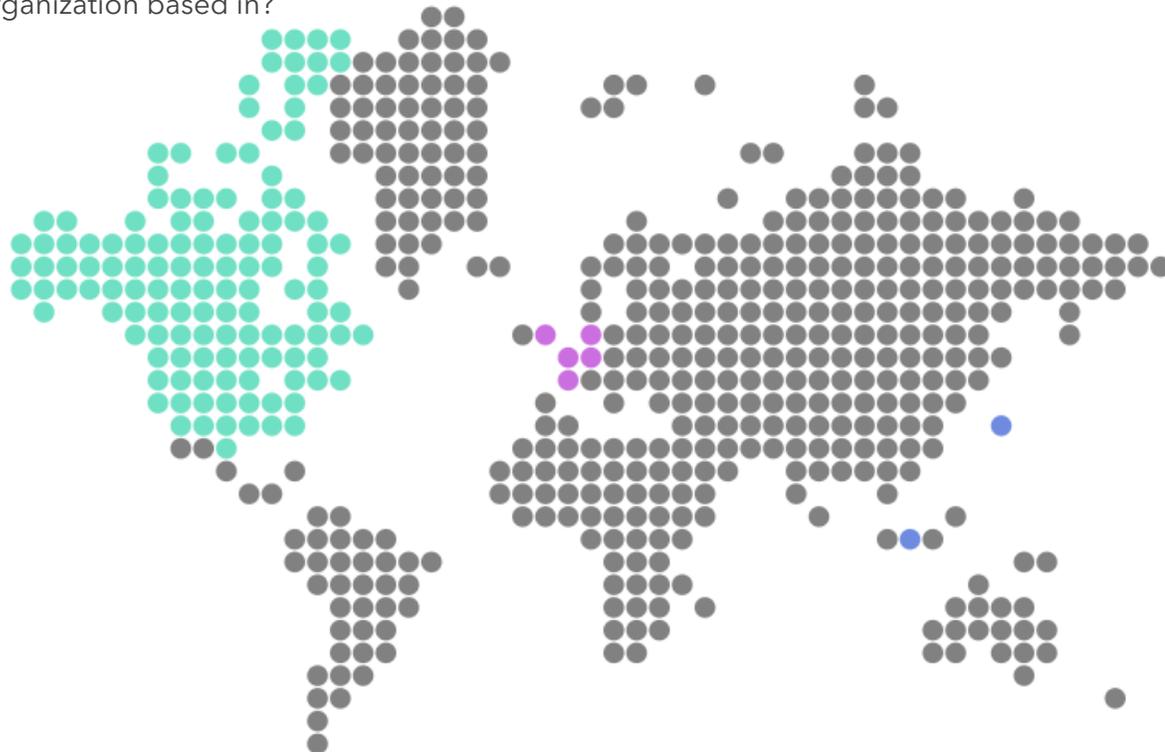


Fieldwork Dates
March - April 2024

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

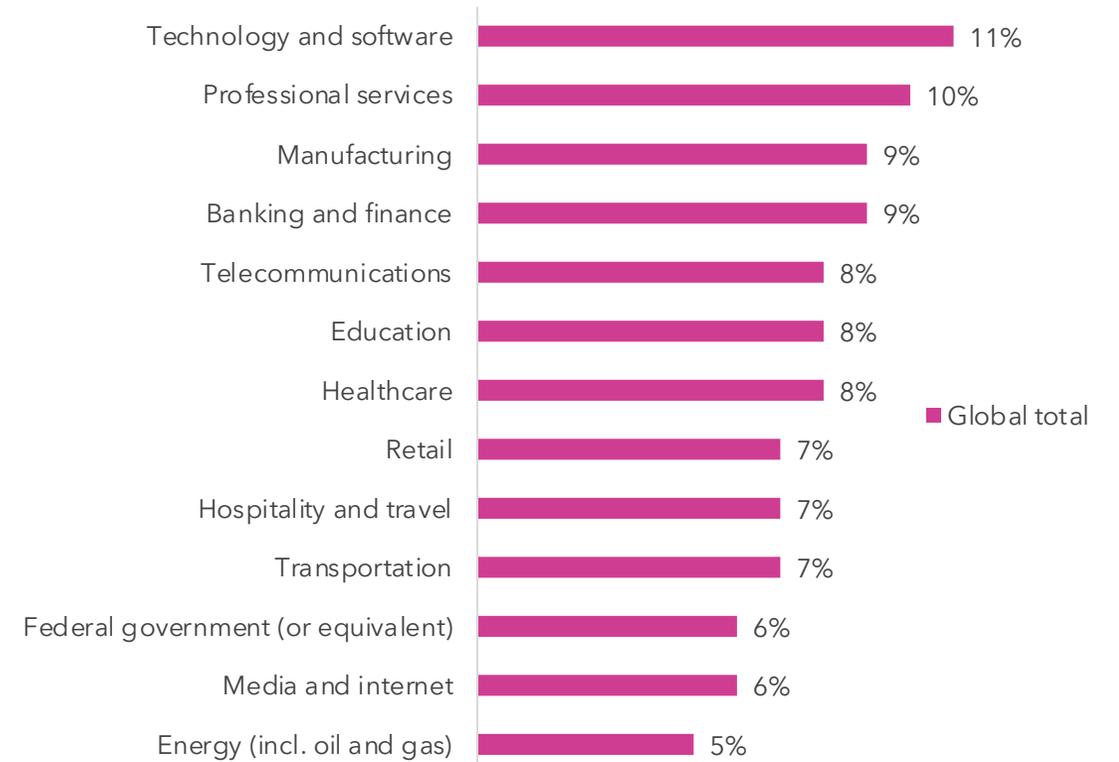
S4. How many employees does your organization have?



Base: Global total (1,000)

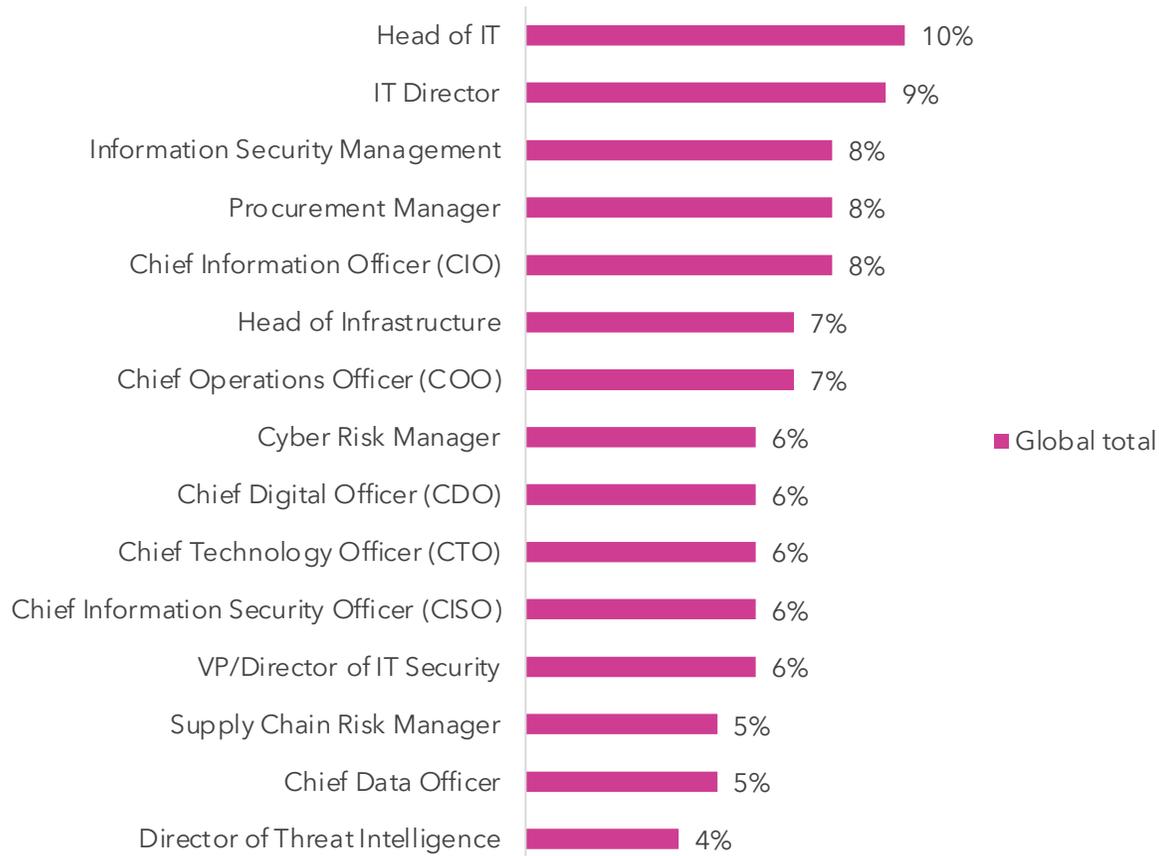
Sector

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



Job title

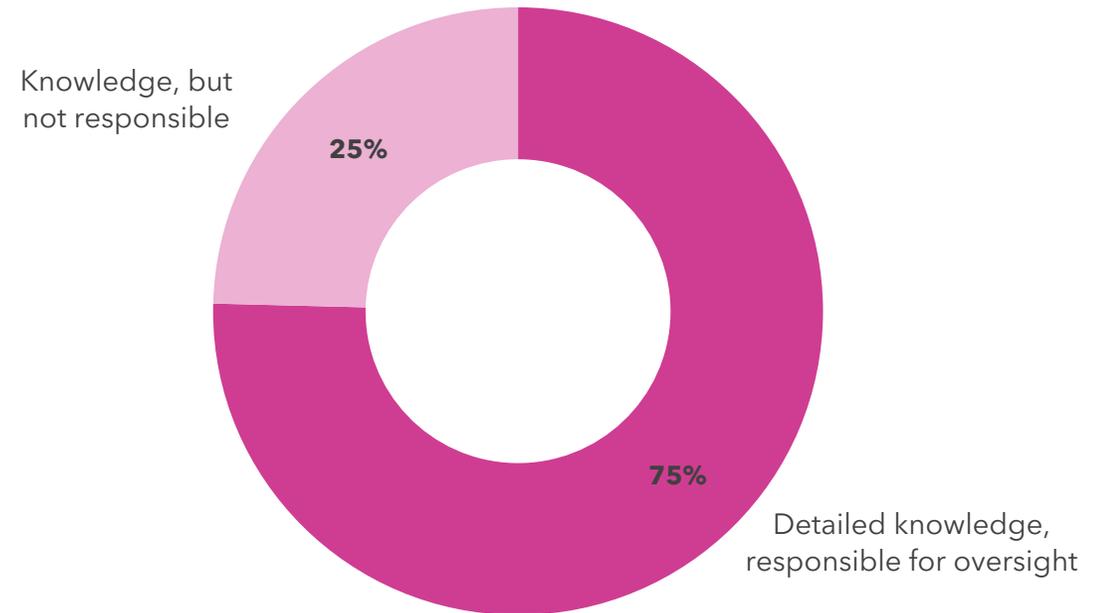
S5. Which of these titles is the closest to your role?



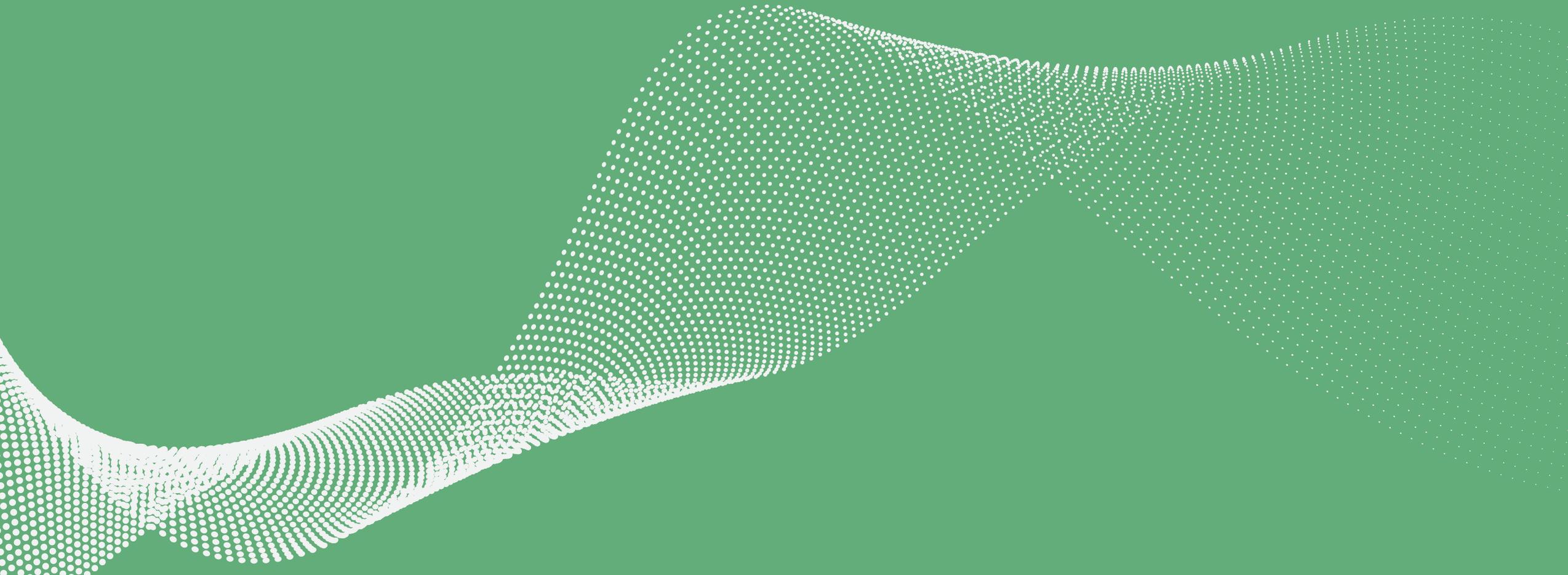
Base: Global total (1,000)

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?

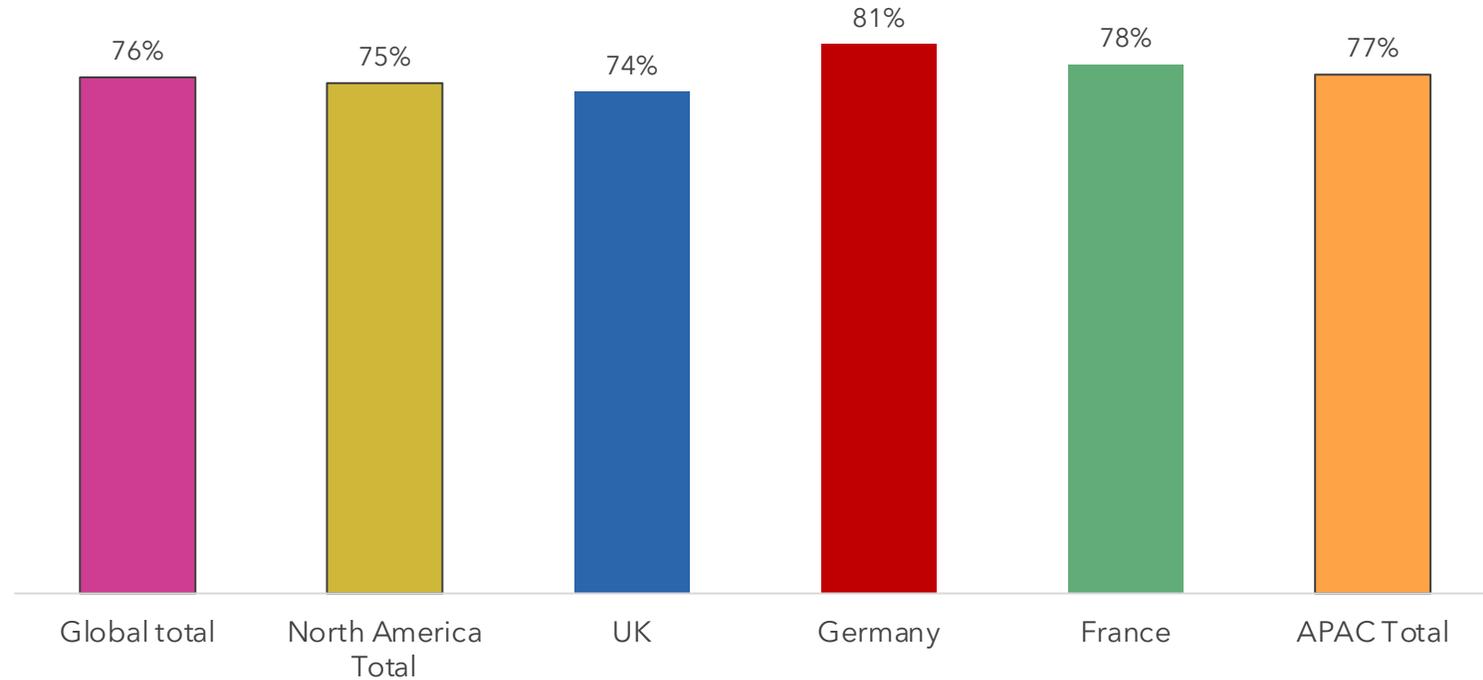


Section 1: Working with suppliers/partners to secure the supply chain of software you consume



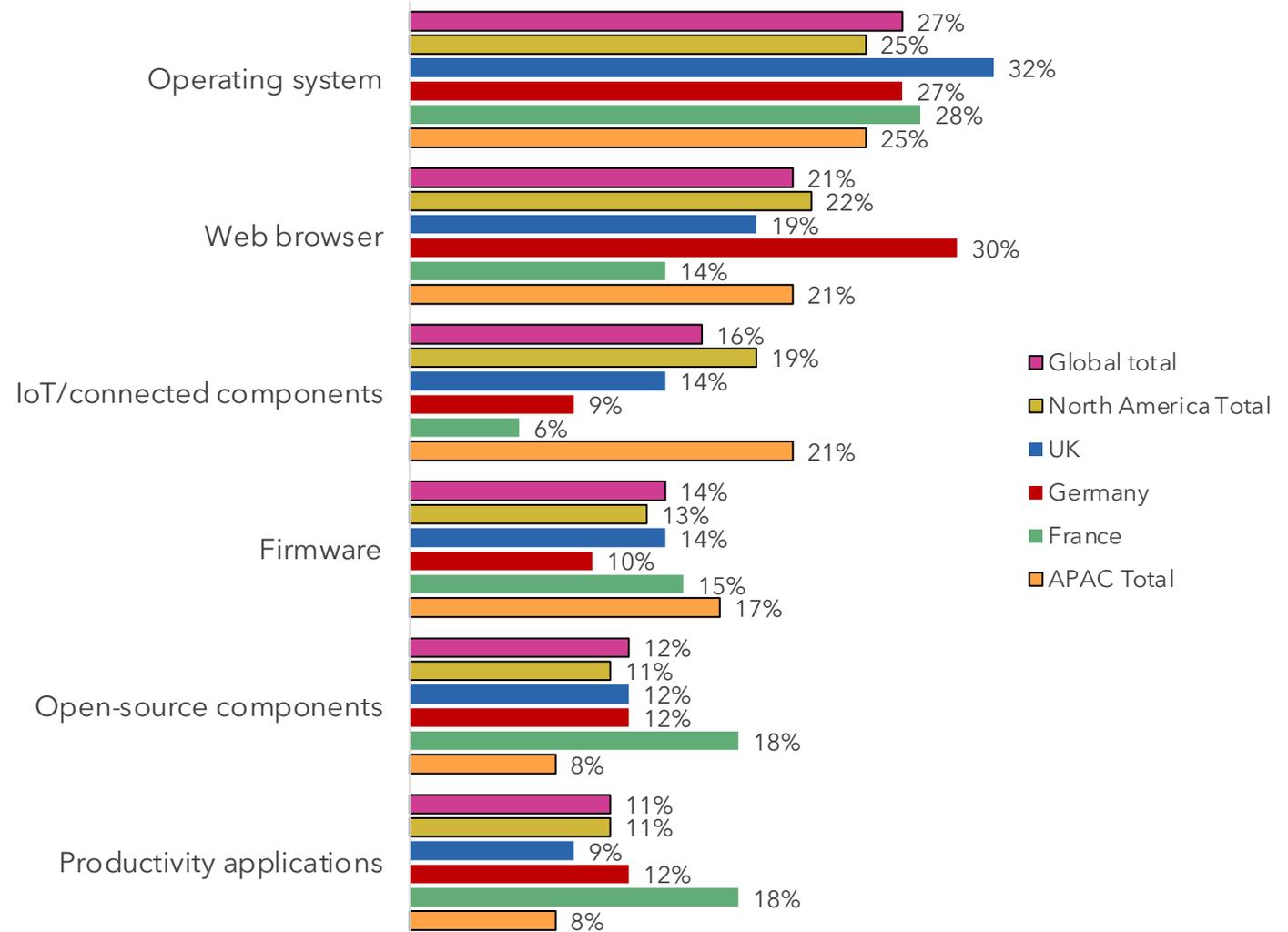
Being notified of a vulnerability or attack within software supply chain in the last 12 months

Yes responses



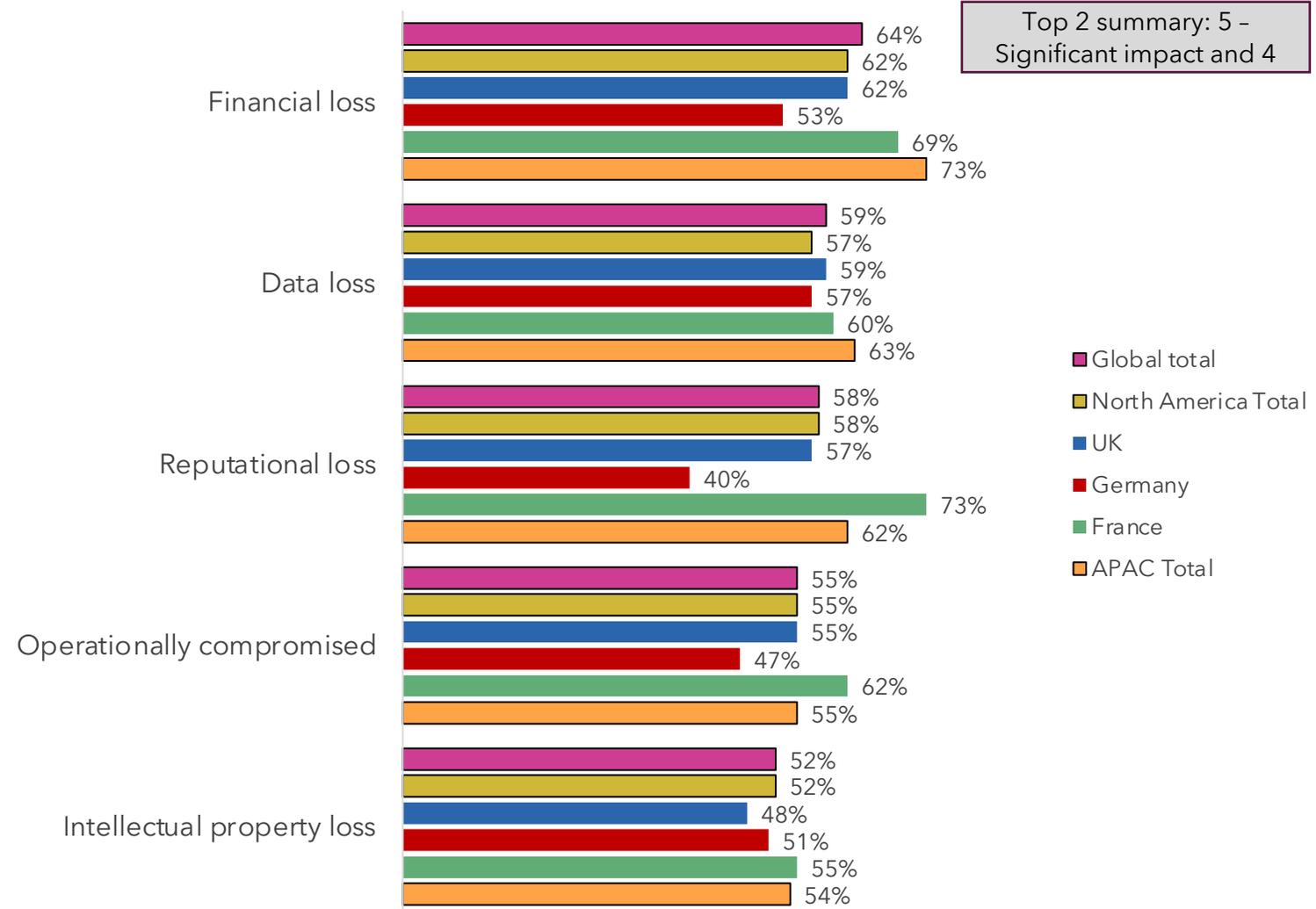
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Vulnerable components having the biggest impact for organization



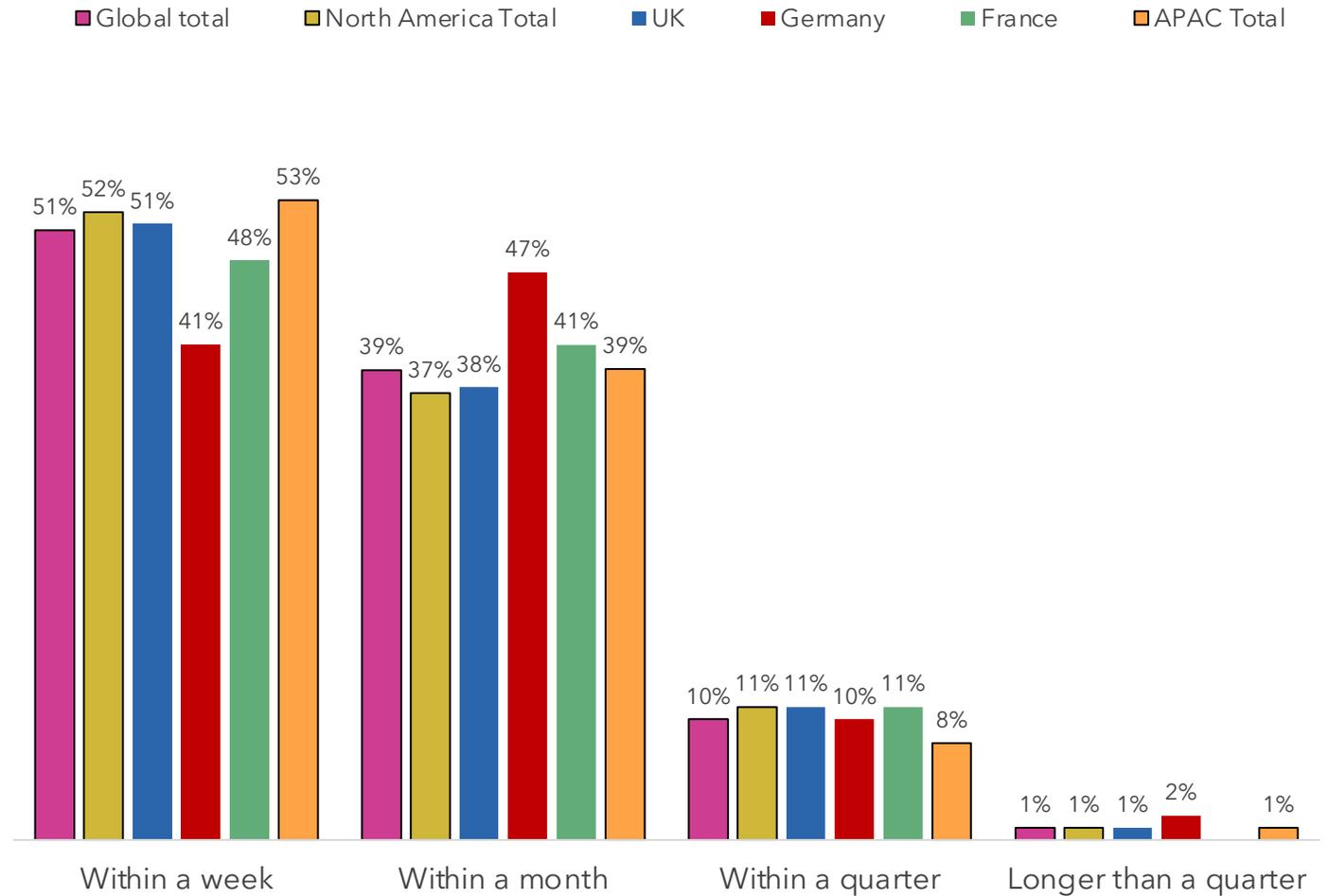
Base: Respondents who have been notified of a vulnerability or attack within their supply chain (761) North America (301) UK (148) Germany (81) France (78) APAC total (153)

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)

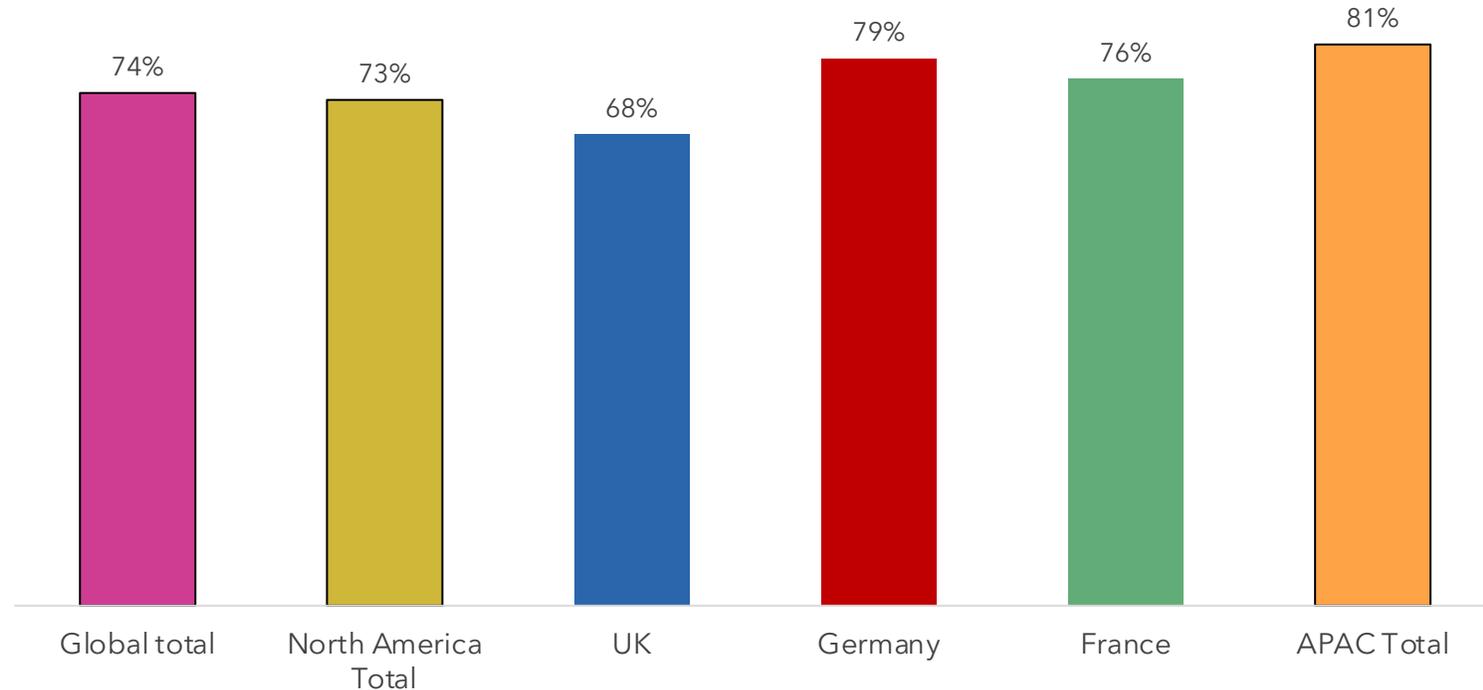
Time taken to fully recover from an exploited vulnerability in software supply chain



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

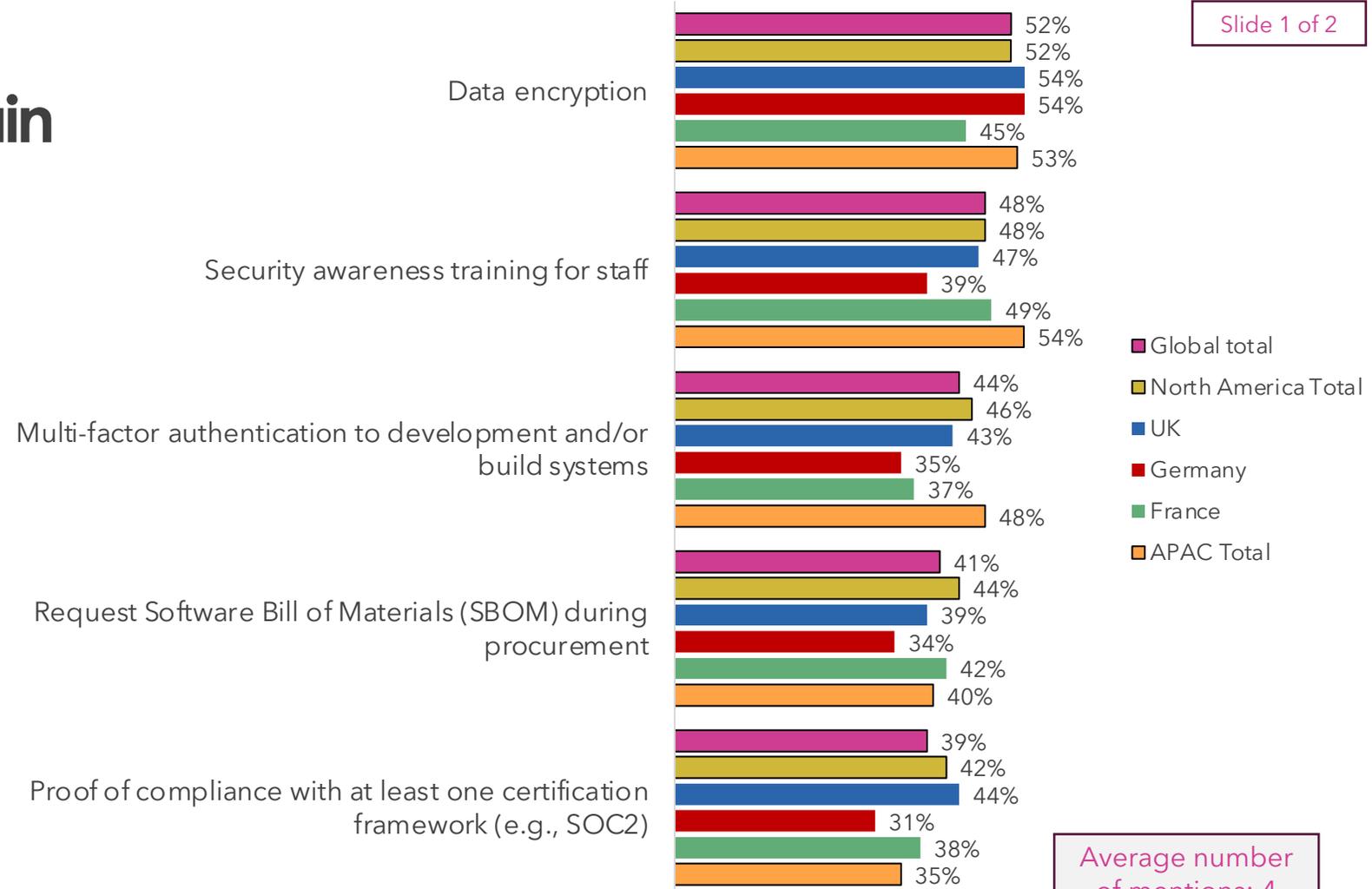
Made aware of a member of supply chain not previously aware of / monitoring for security practices

Yes responses



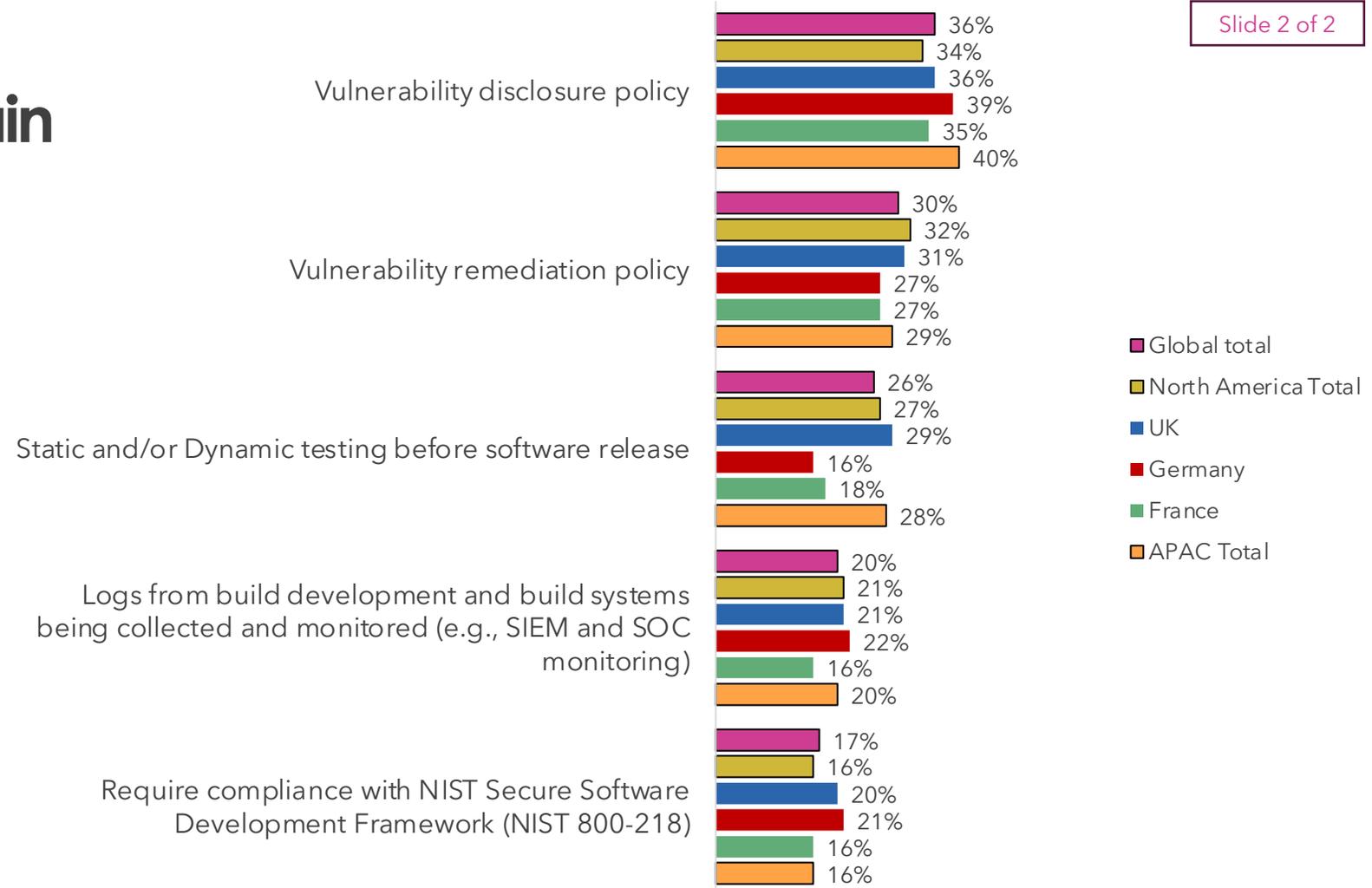
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Measures insist supply chain has in place



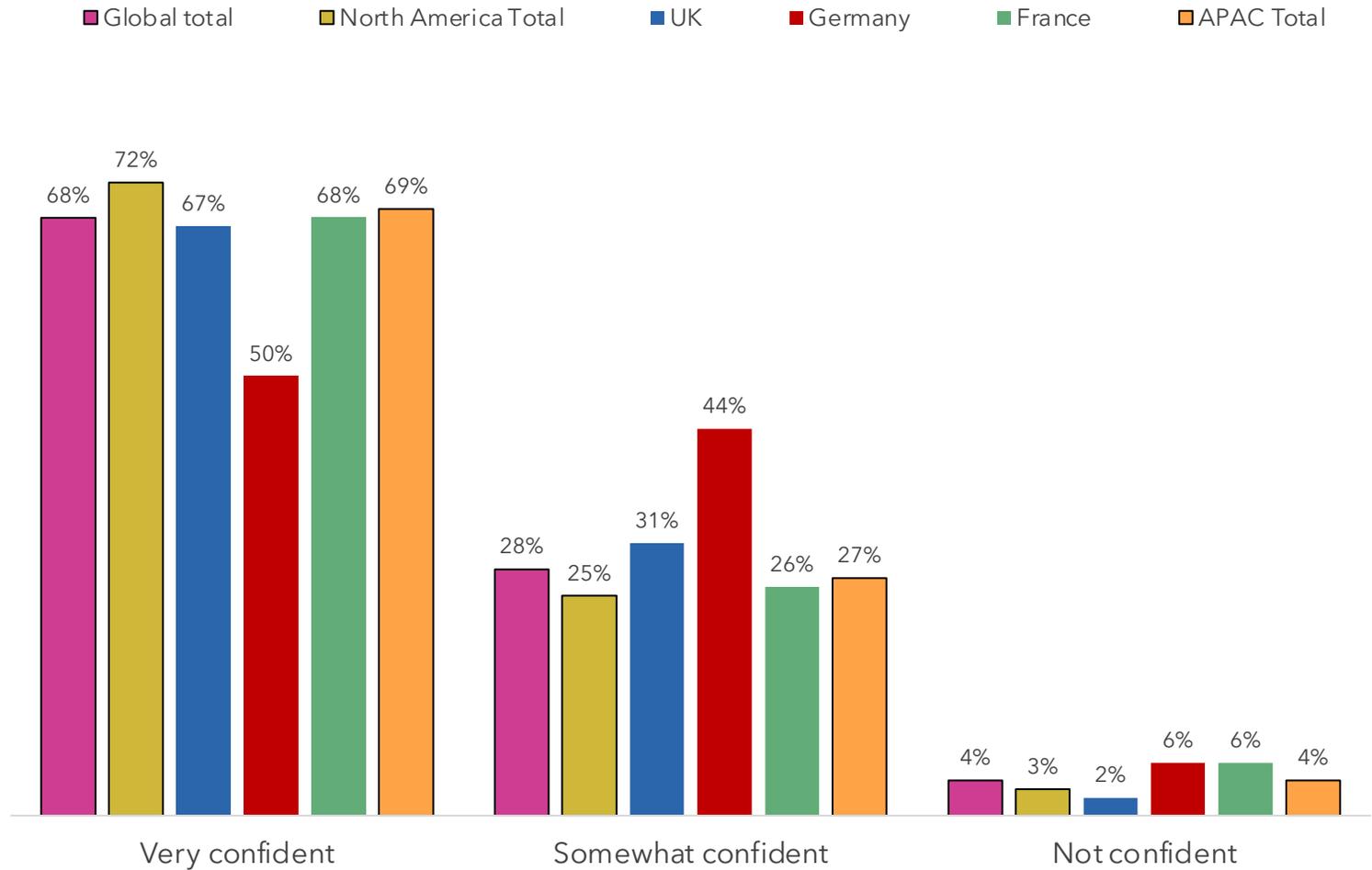
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Measures insist supply chain has in place



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

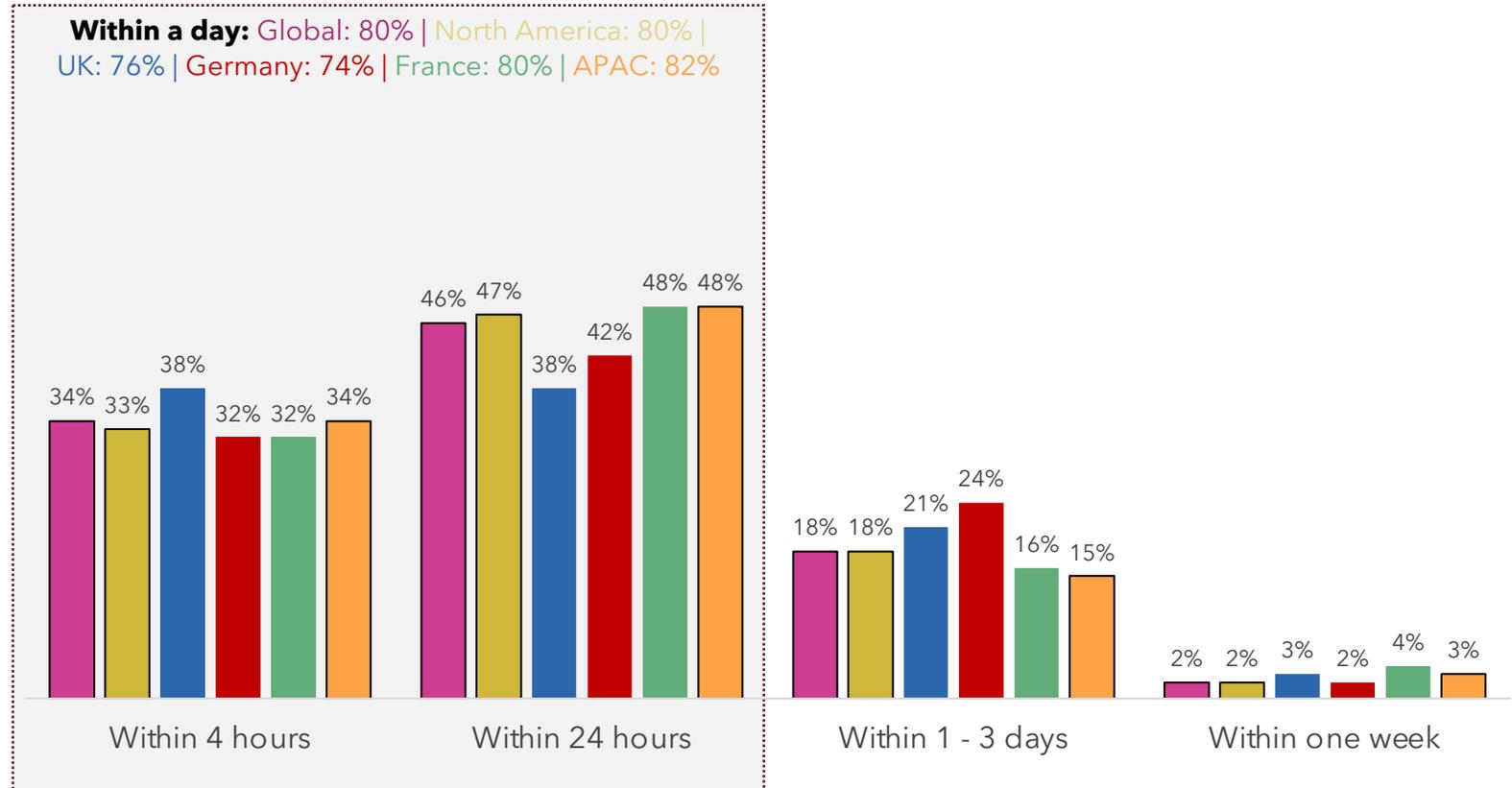
Confidence that suppliers / partners can identify and prevent a vulnerability



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

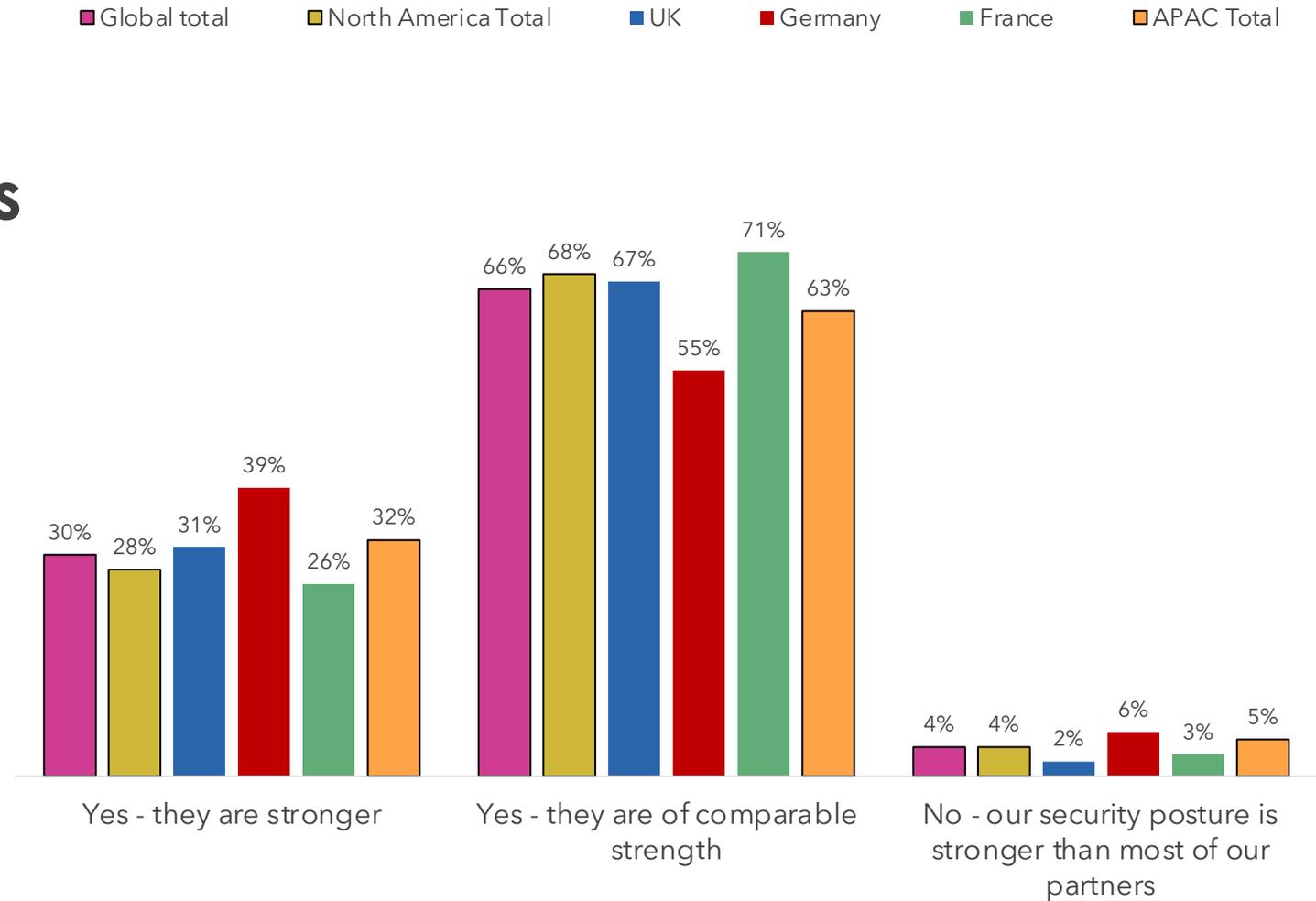
Expected time taken to be notified in the event of a supplier / partner suffering a cyber breach

Global total North America Total UK Germany France APAC Total



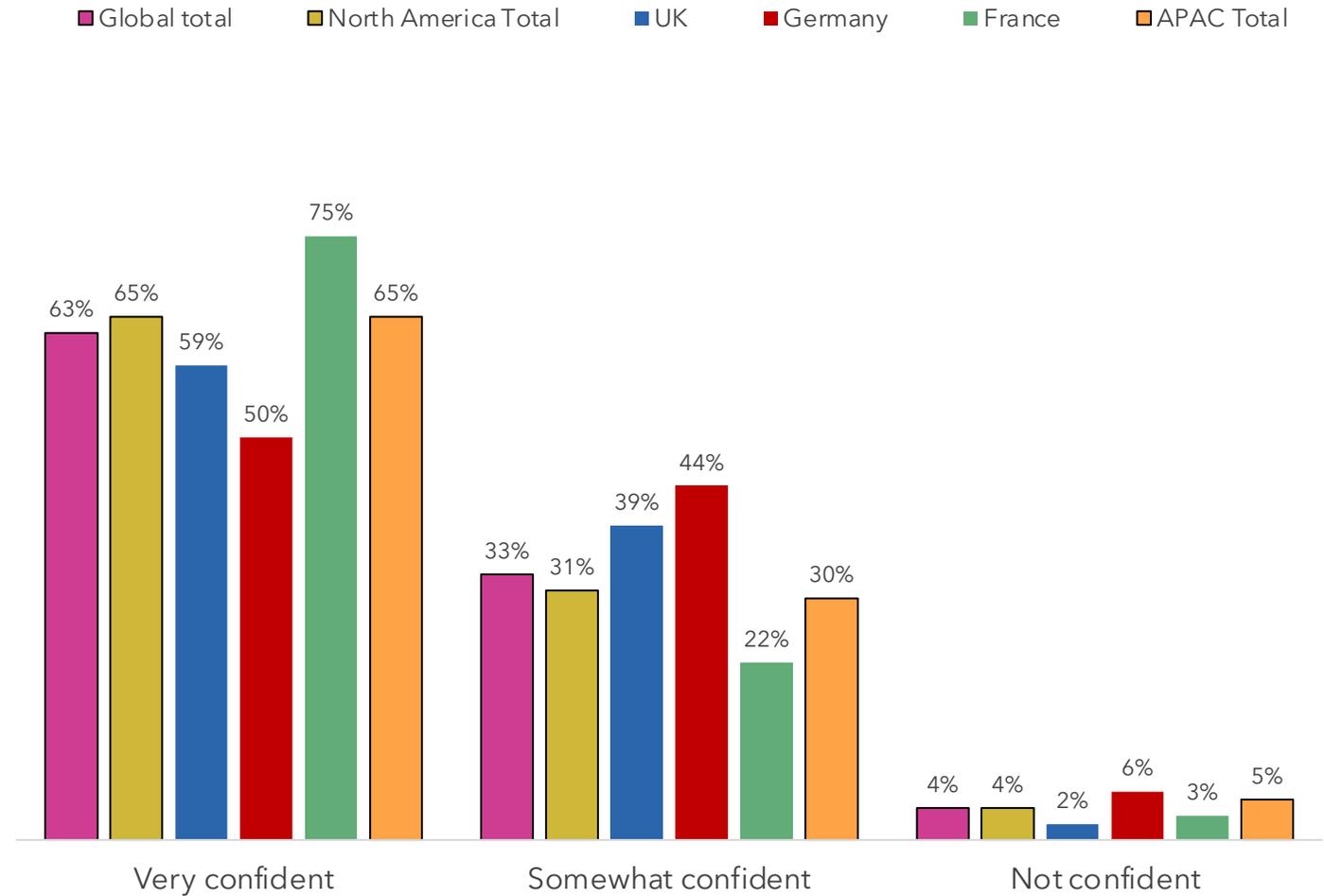
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Comparability of suppliers / partners cybersecurity policies



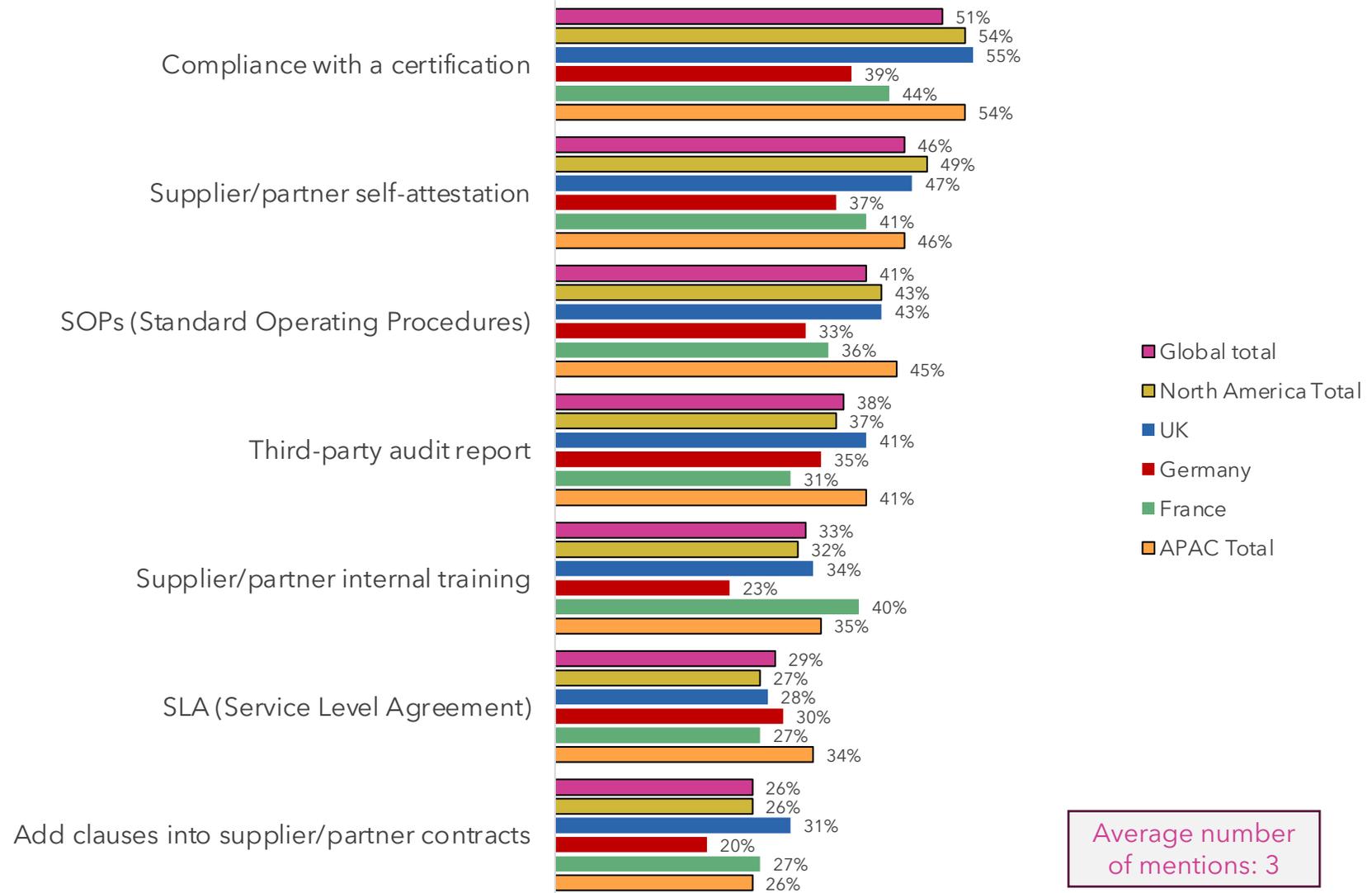
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

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)

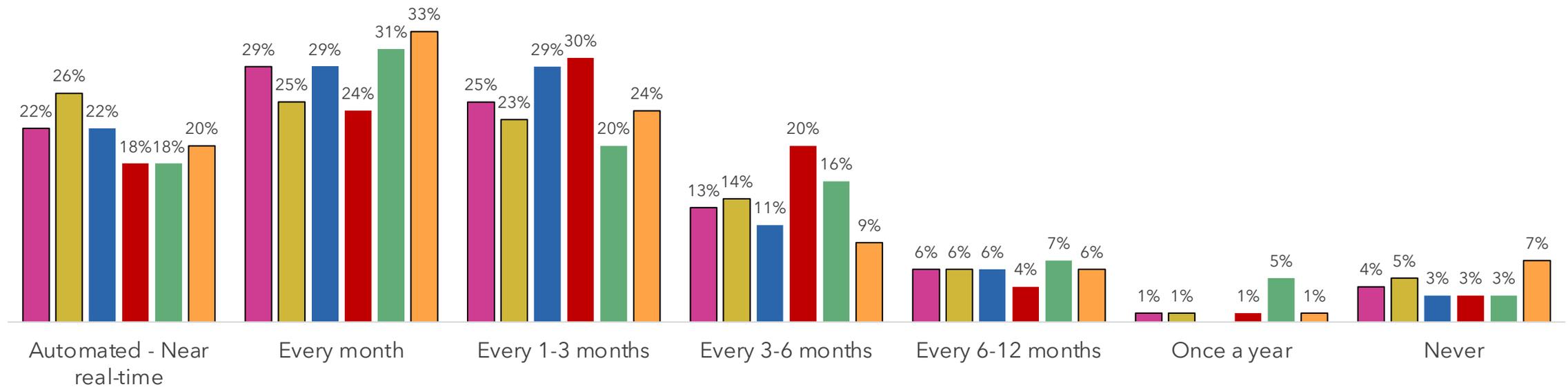
Evidence required for suppliers / partners to attest level of securing software supply chain



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

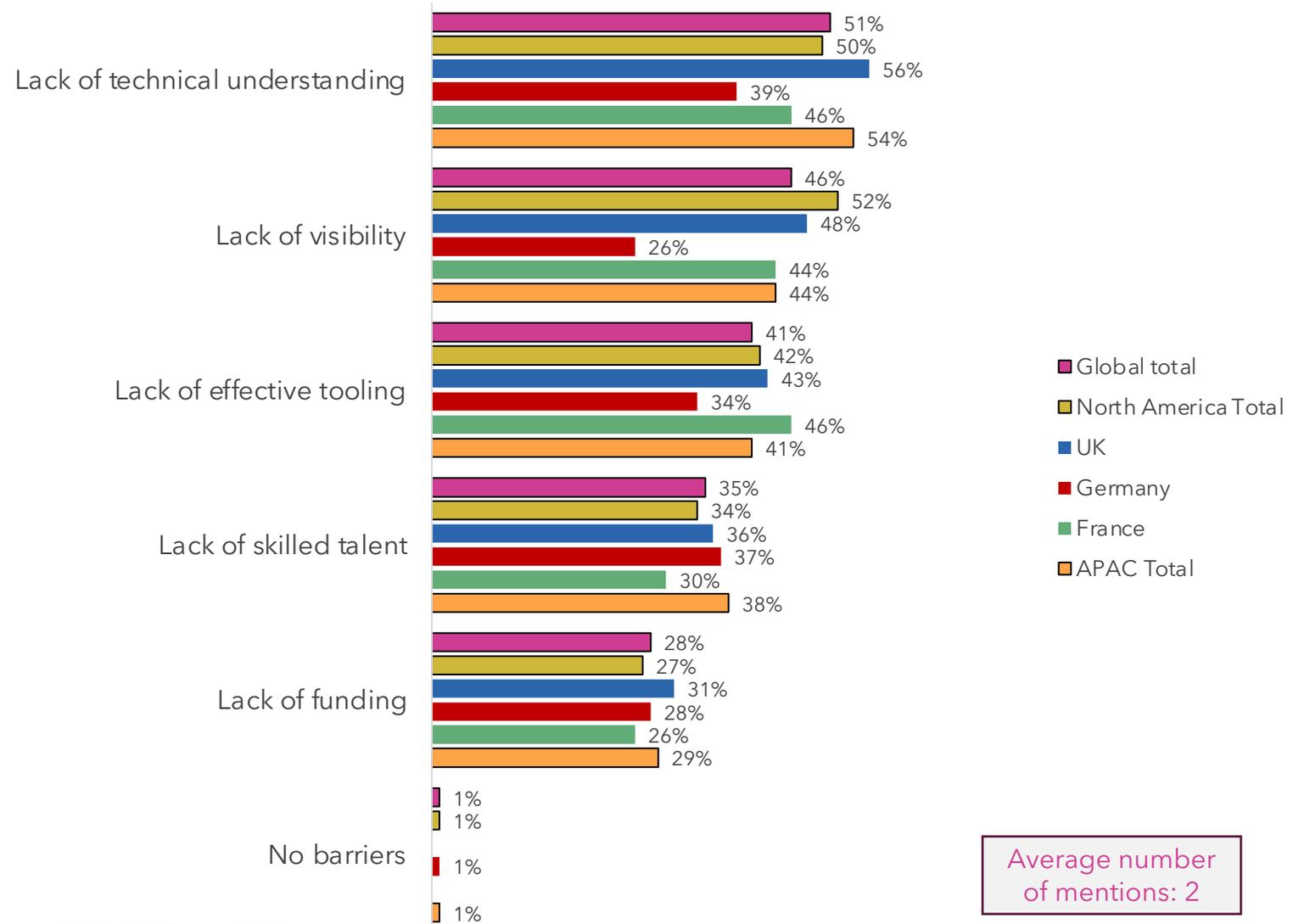
Global total North America Total UK Germany France APAC Total

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)

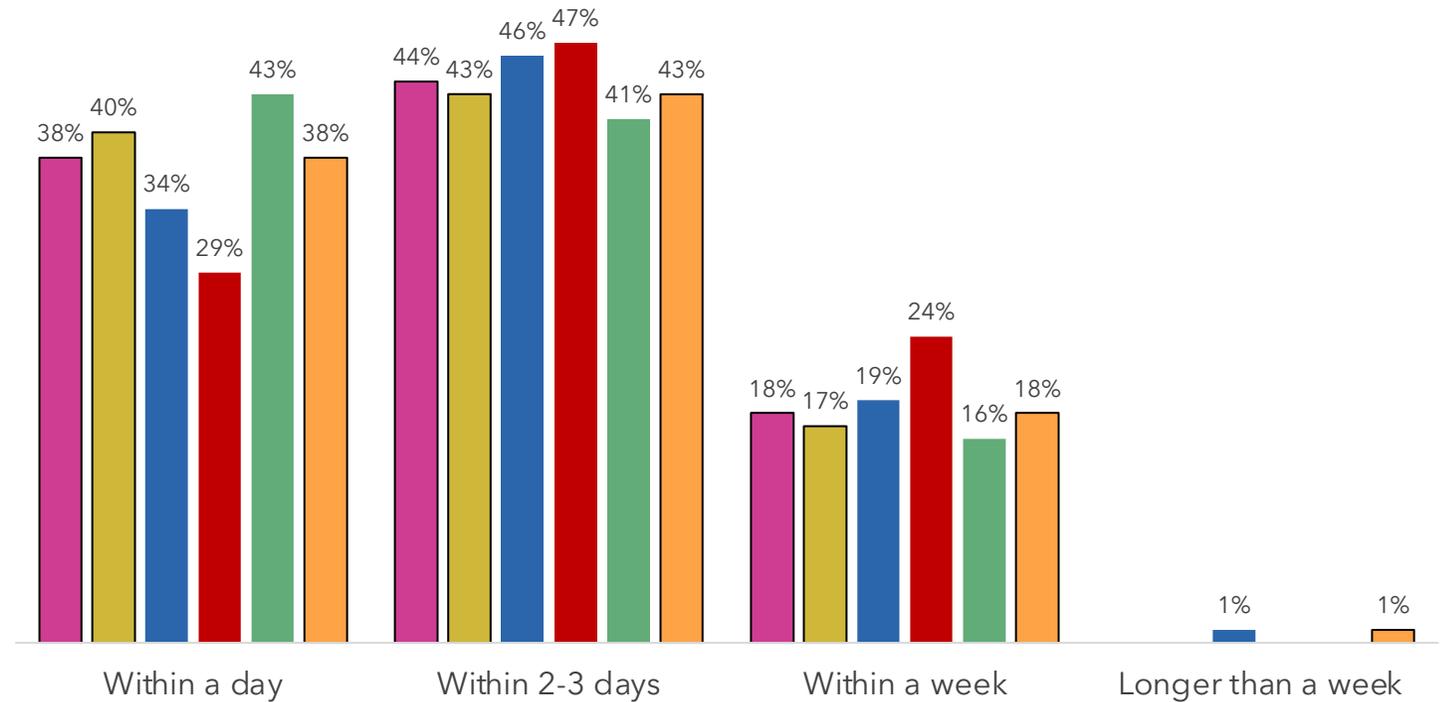
Biggest barriers to regular software inventories



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

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

Global total North America Total UK Germany France APAC Total

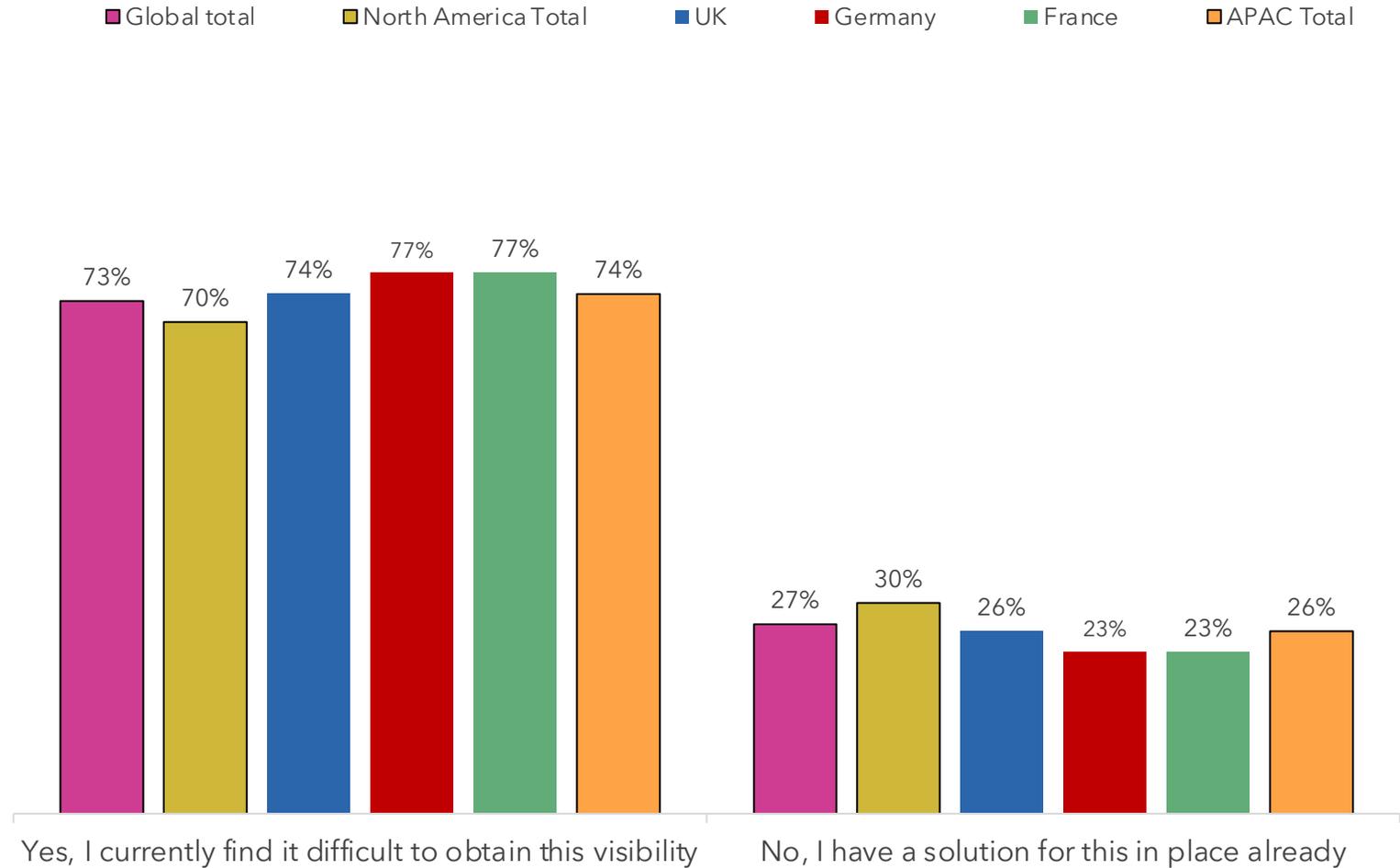


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Single coded question

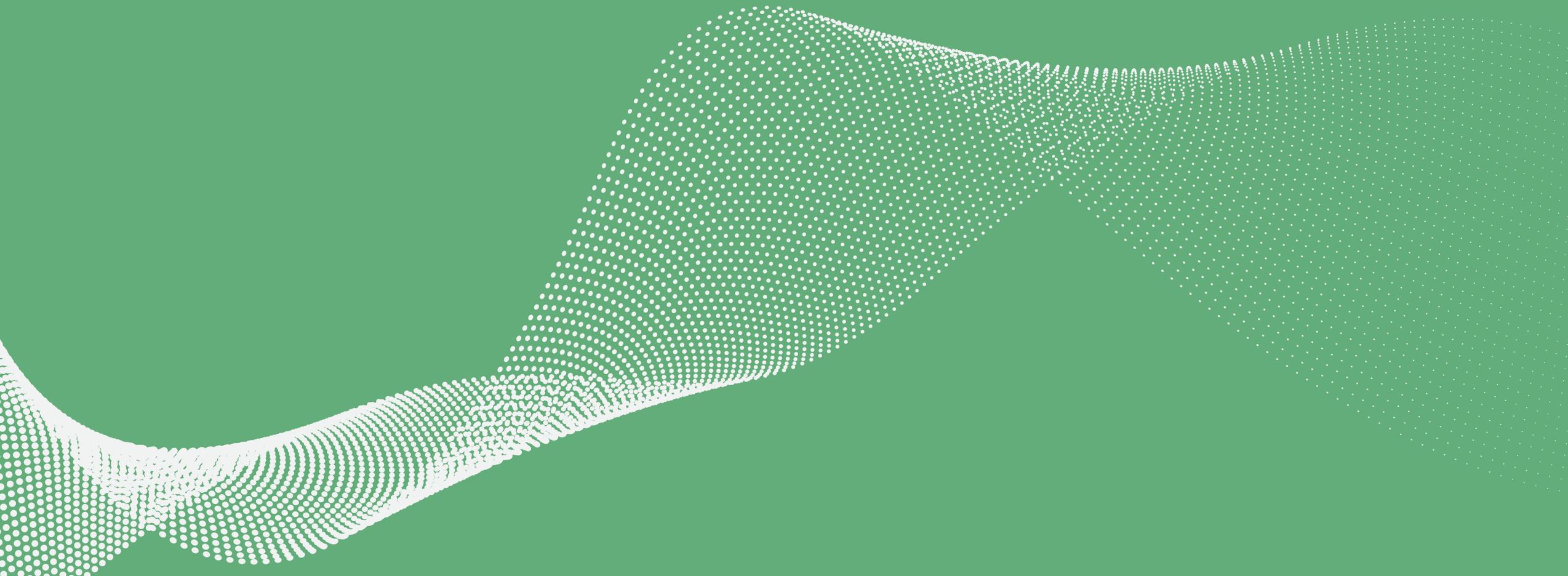
Q14. You have become aware of a vulnerability that may impact the supply chain of software you consume. From the time you start your investigation, on average, how long does it take your organization to identify if an impacted library is used in any of the software you consume?

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



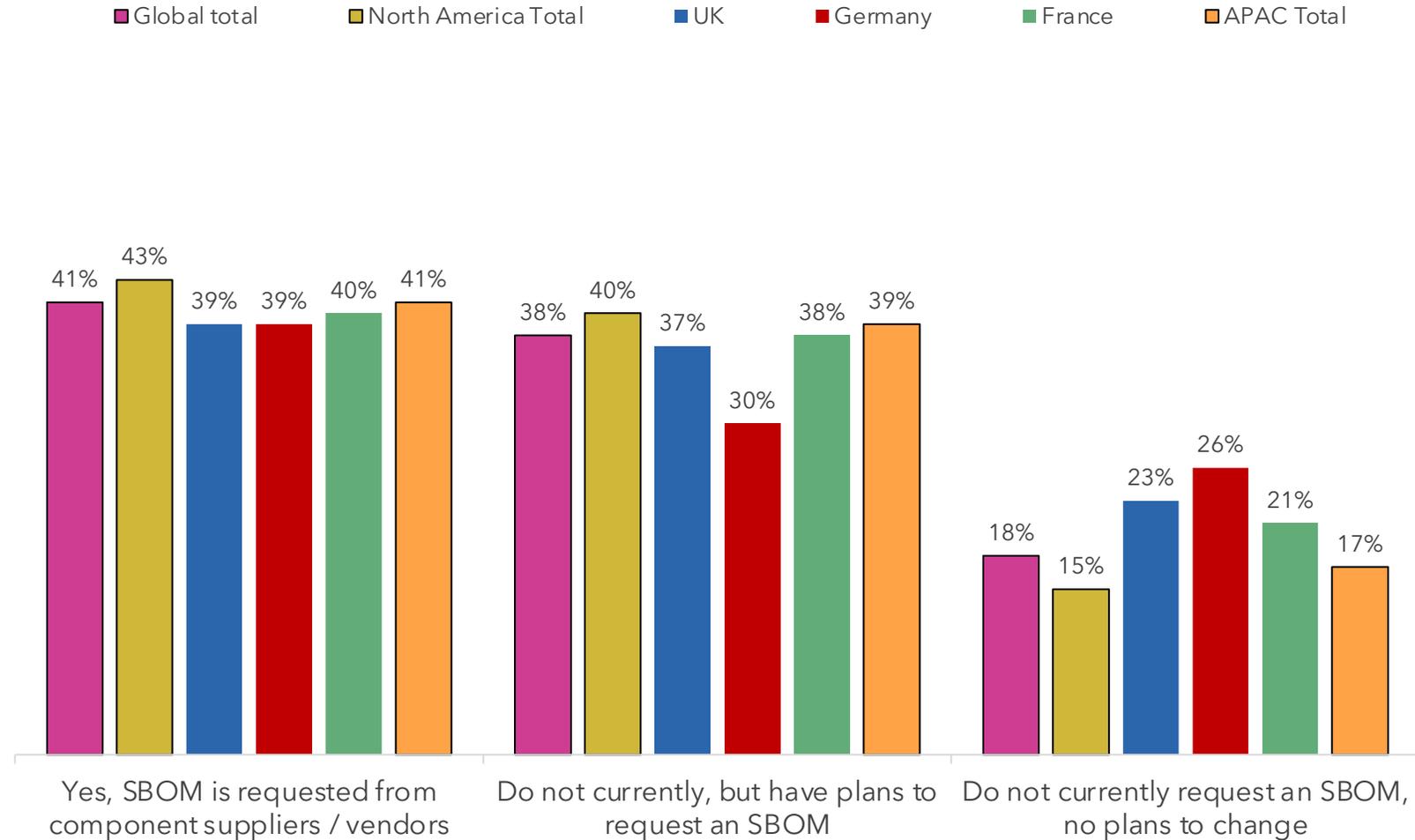
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Section 2: Regulations and compliance



Requests for a Software Bill of Materials (SBOM):

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

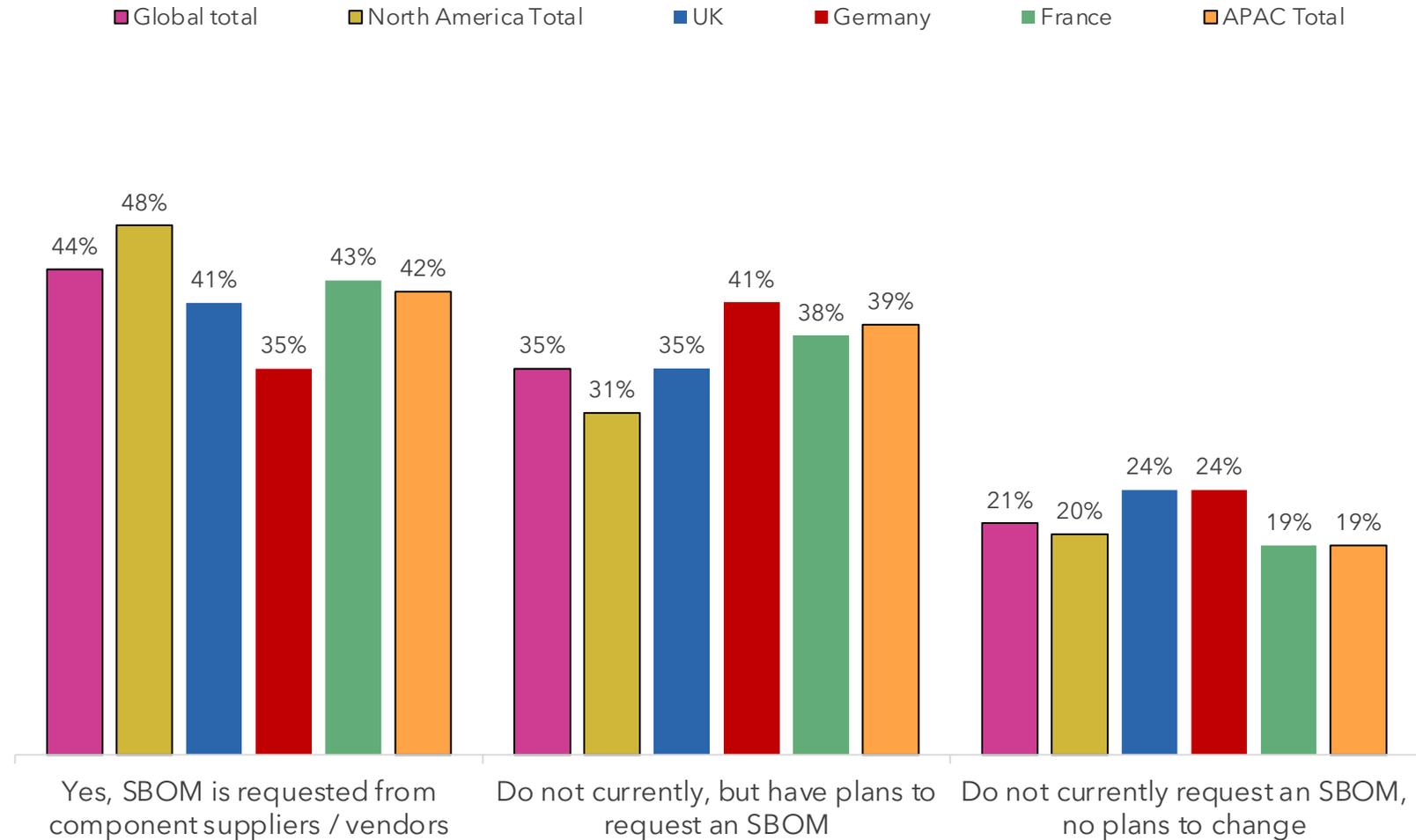


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

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

Requests for a Software Bill of Materials (SBOM):

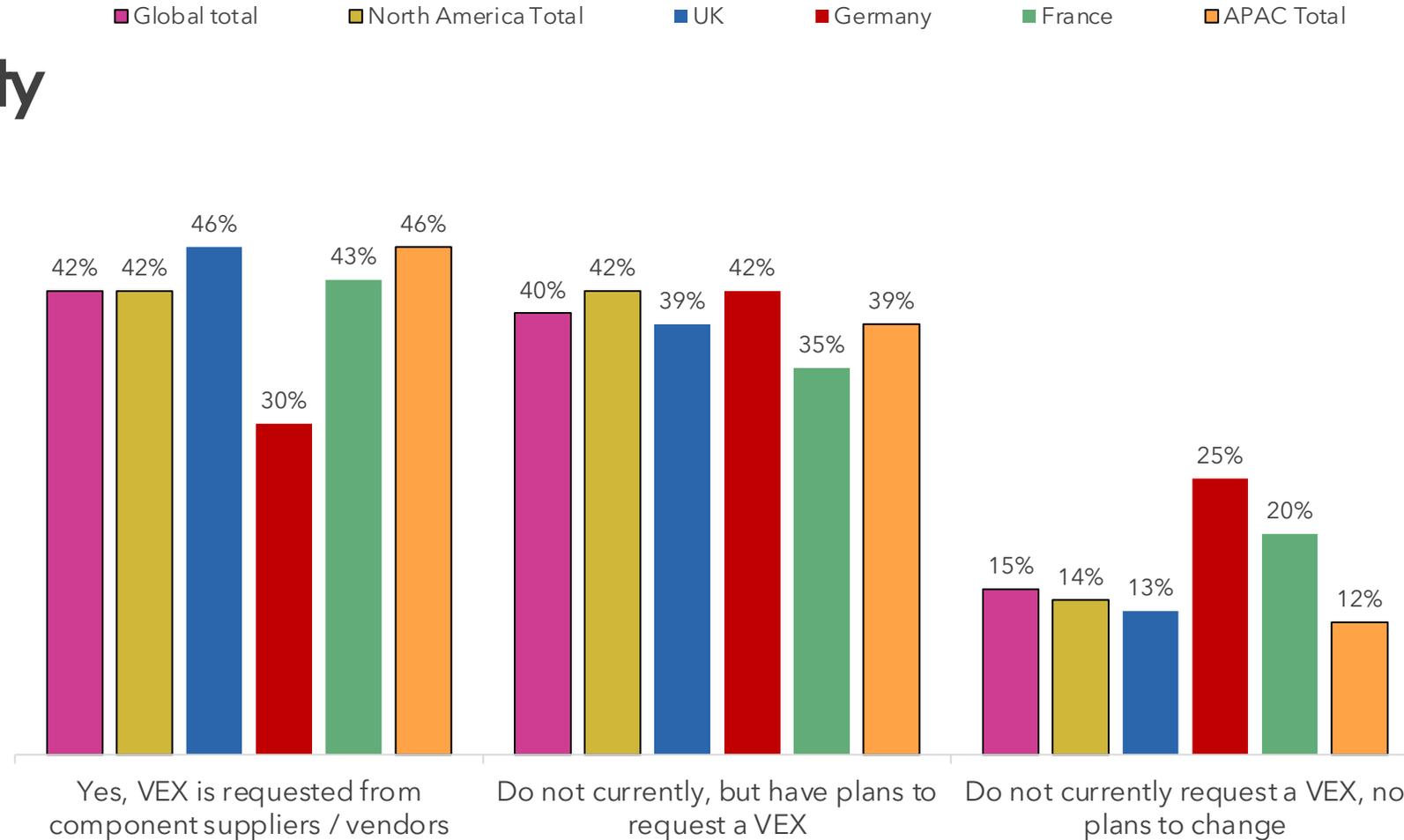
from vendors that you purchase software from, for use within your organization?



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

Requests for a Vulnerability Exploitability eXchange (VEX) artifact:

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

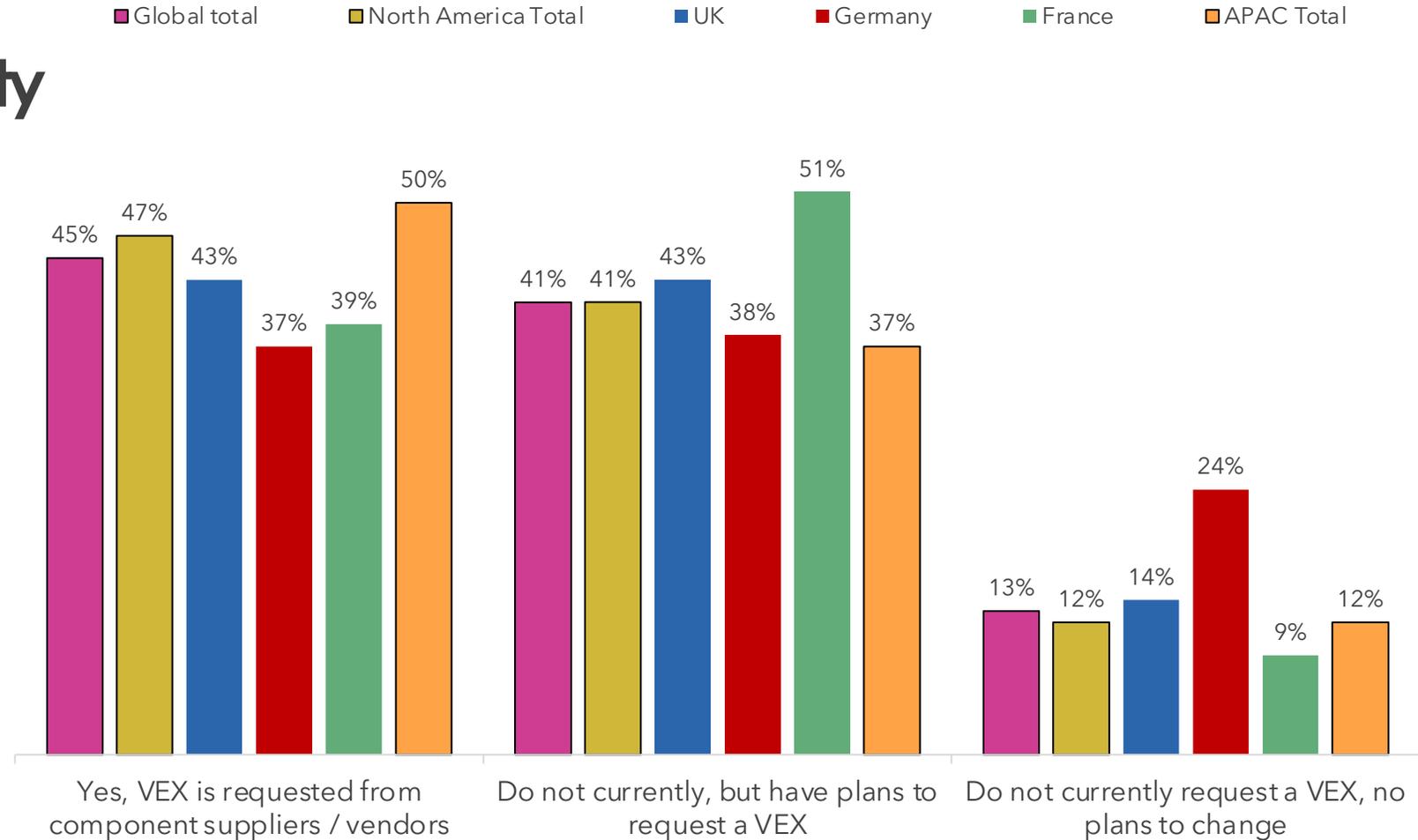


Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

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

Requests for a Vulnerability Exploitability eXchange (VEX) artifact:

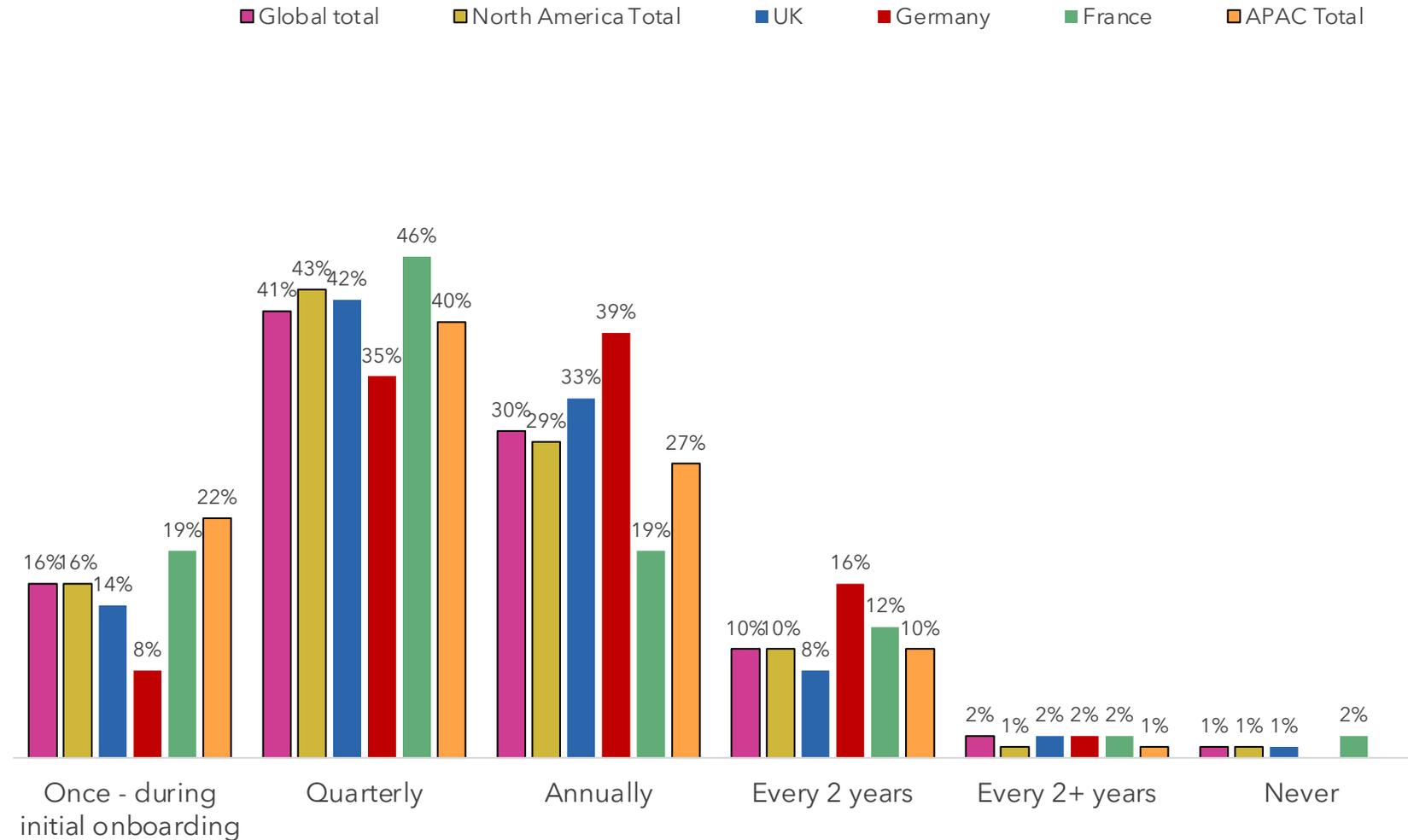
from vendors that you purchase software from, for use within your organization?



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

1% N/A / Don't now

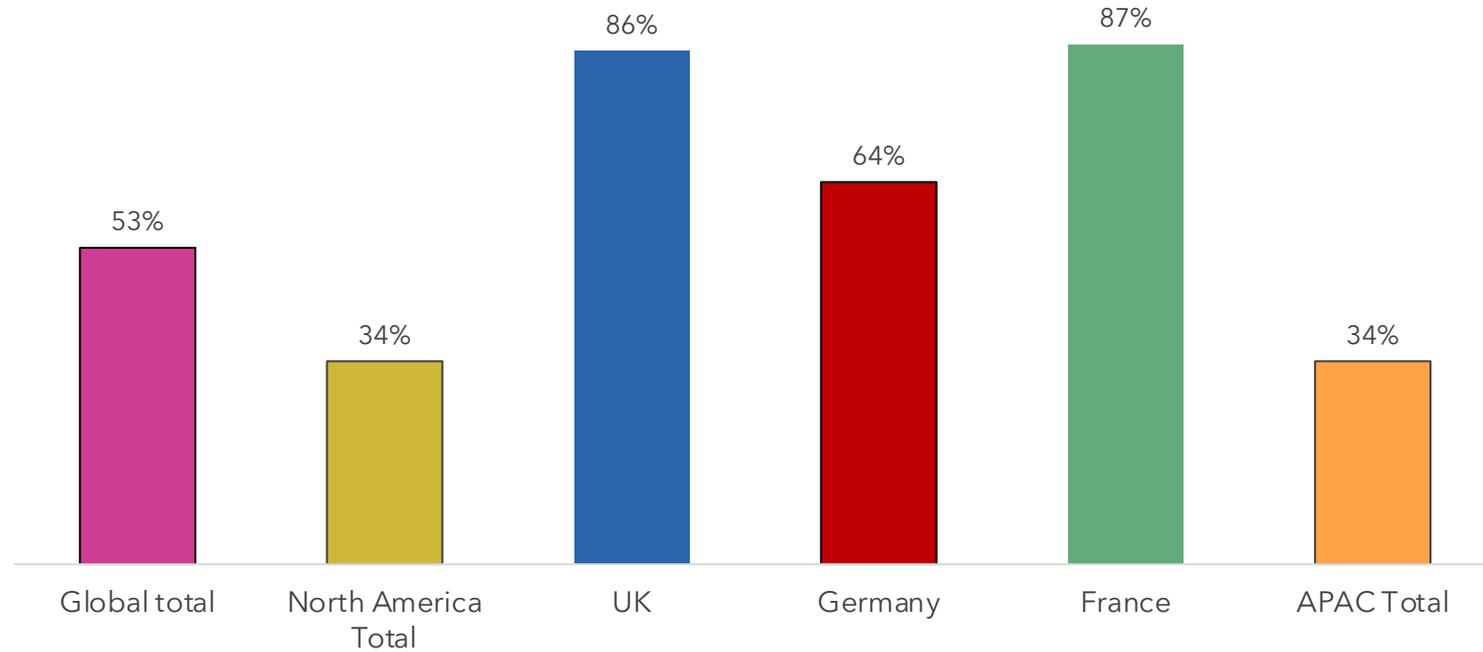
Frequency of suppliers/ partners to provide evidence of compliance to security certifications and frameworks



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

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

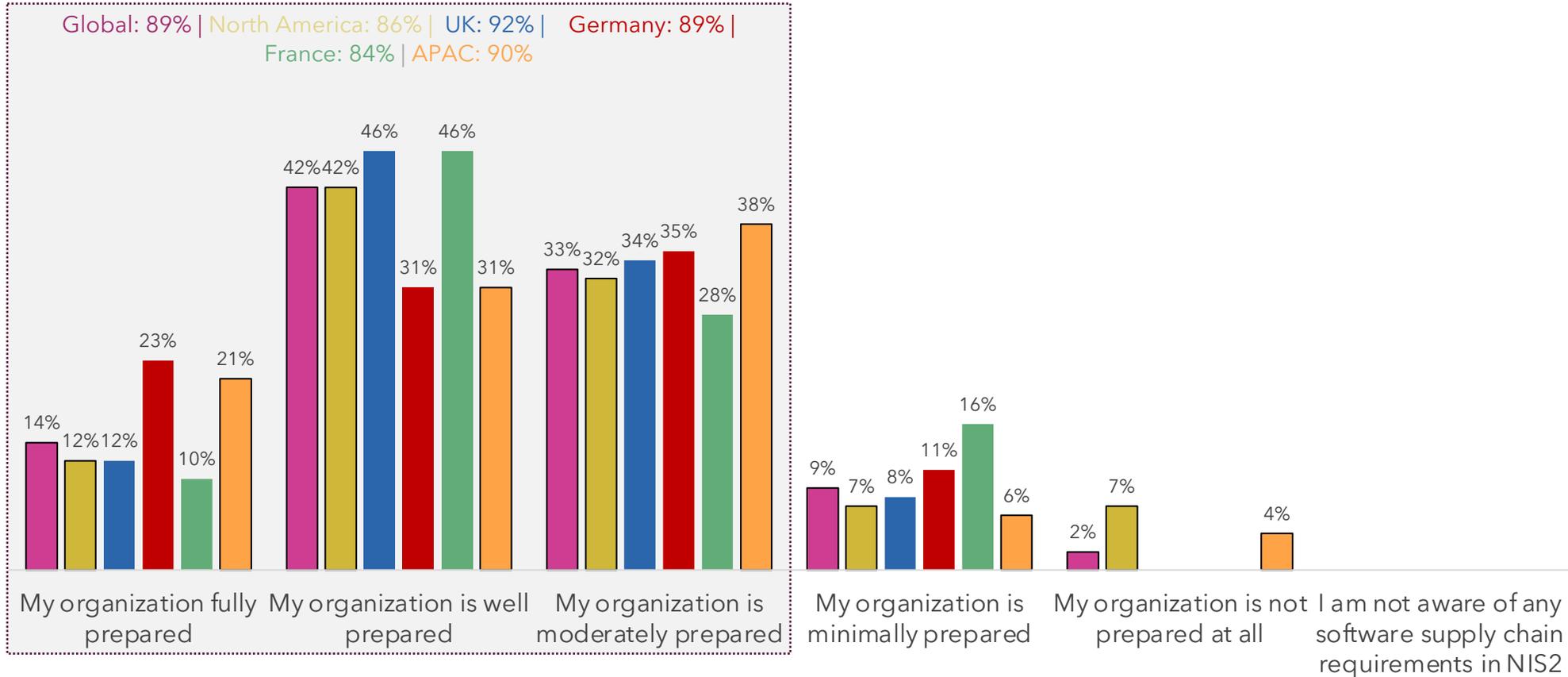
Yes responses



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

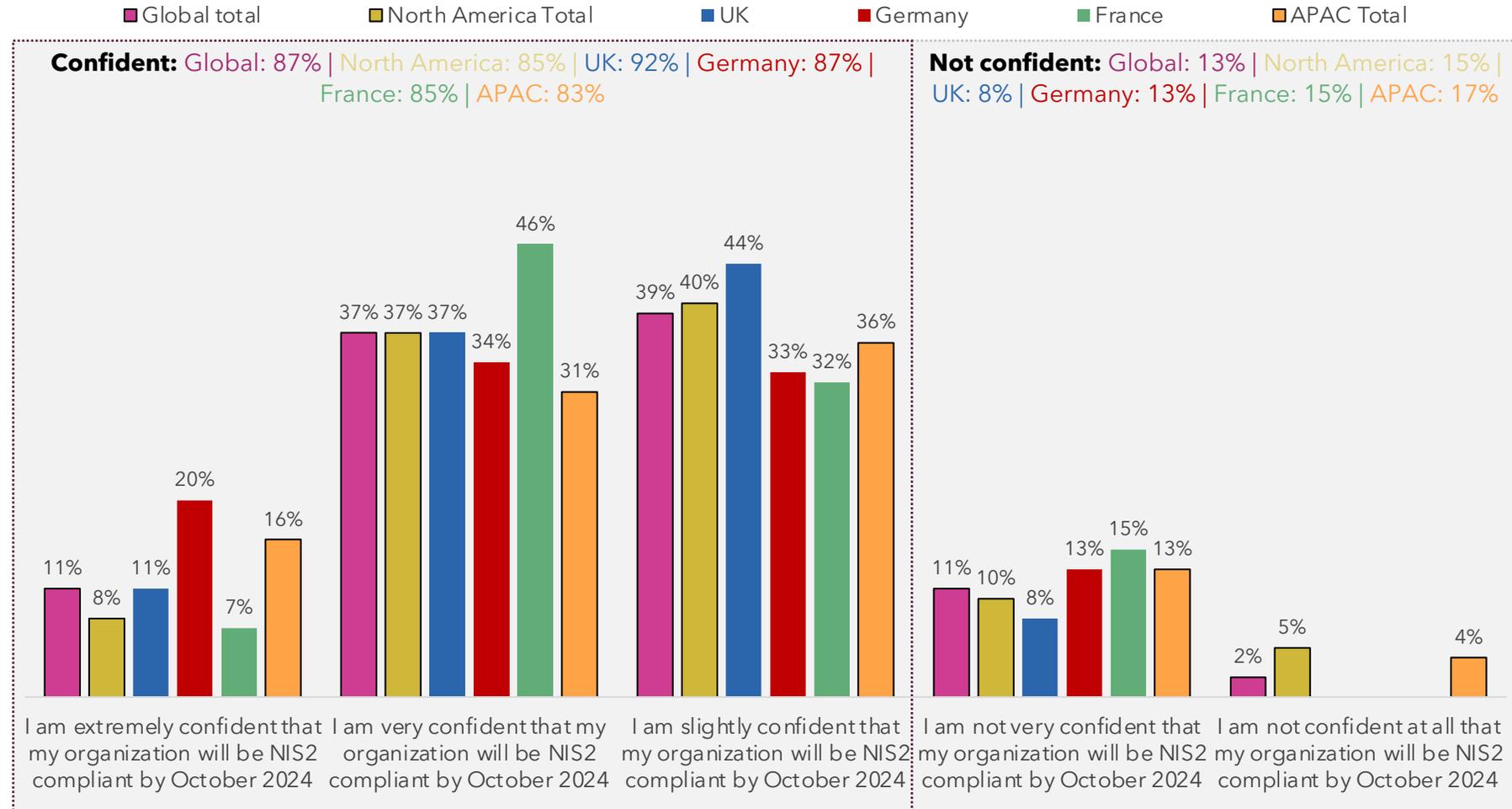
Preparedness for NIS2 compliance relating to security of software supply chains

Global total North America Total UK Germany France APAC Total



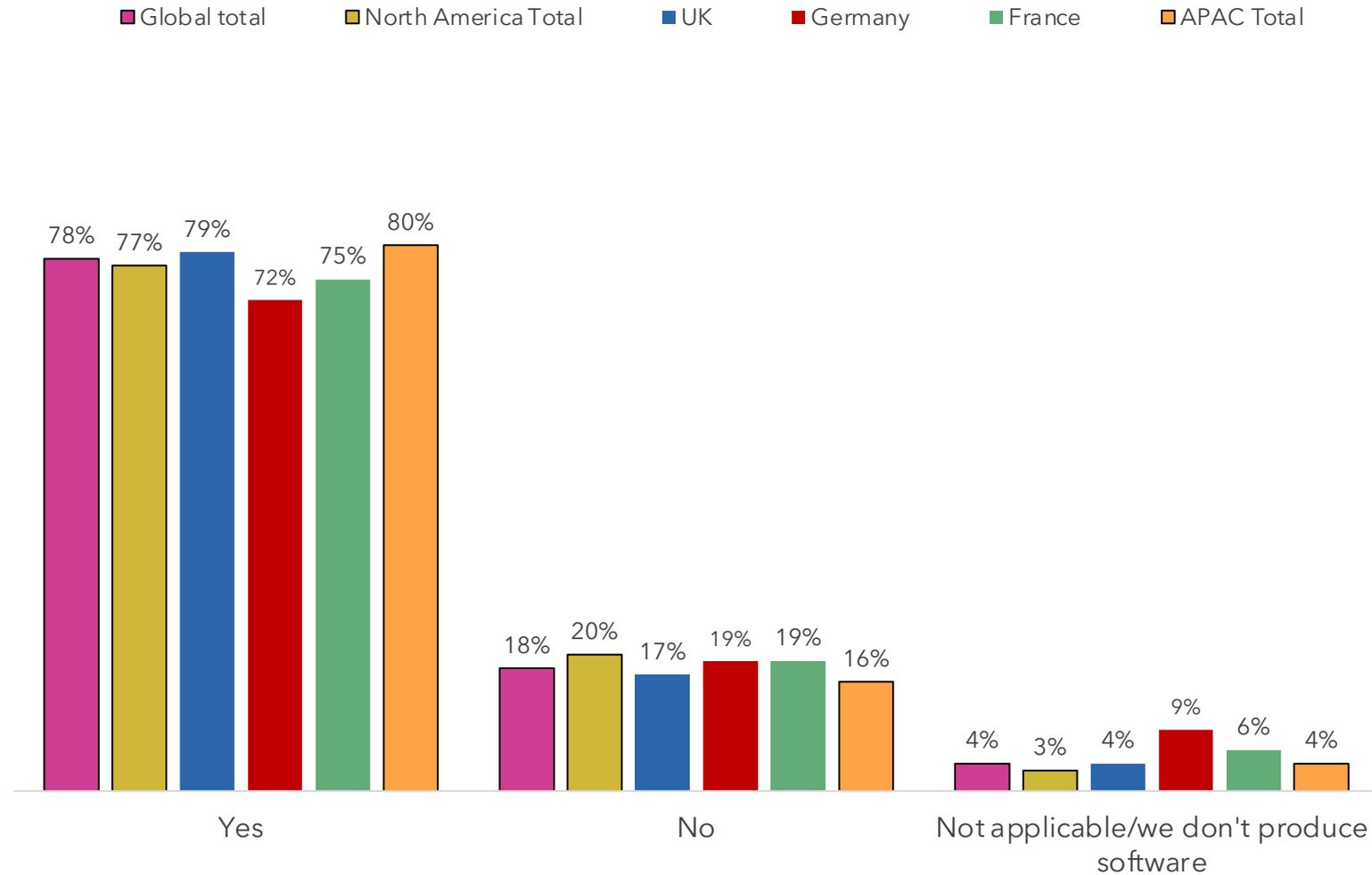
Base: Organizations that are required to adhere to the NIS2 Directive (525) North America (135) UK (171) Germany (64) France (87) APAC total (68)

Confidence that organization will be NIS2 compliant by October 2024 deadline



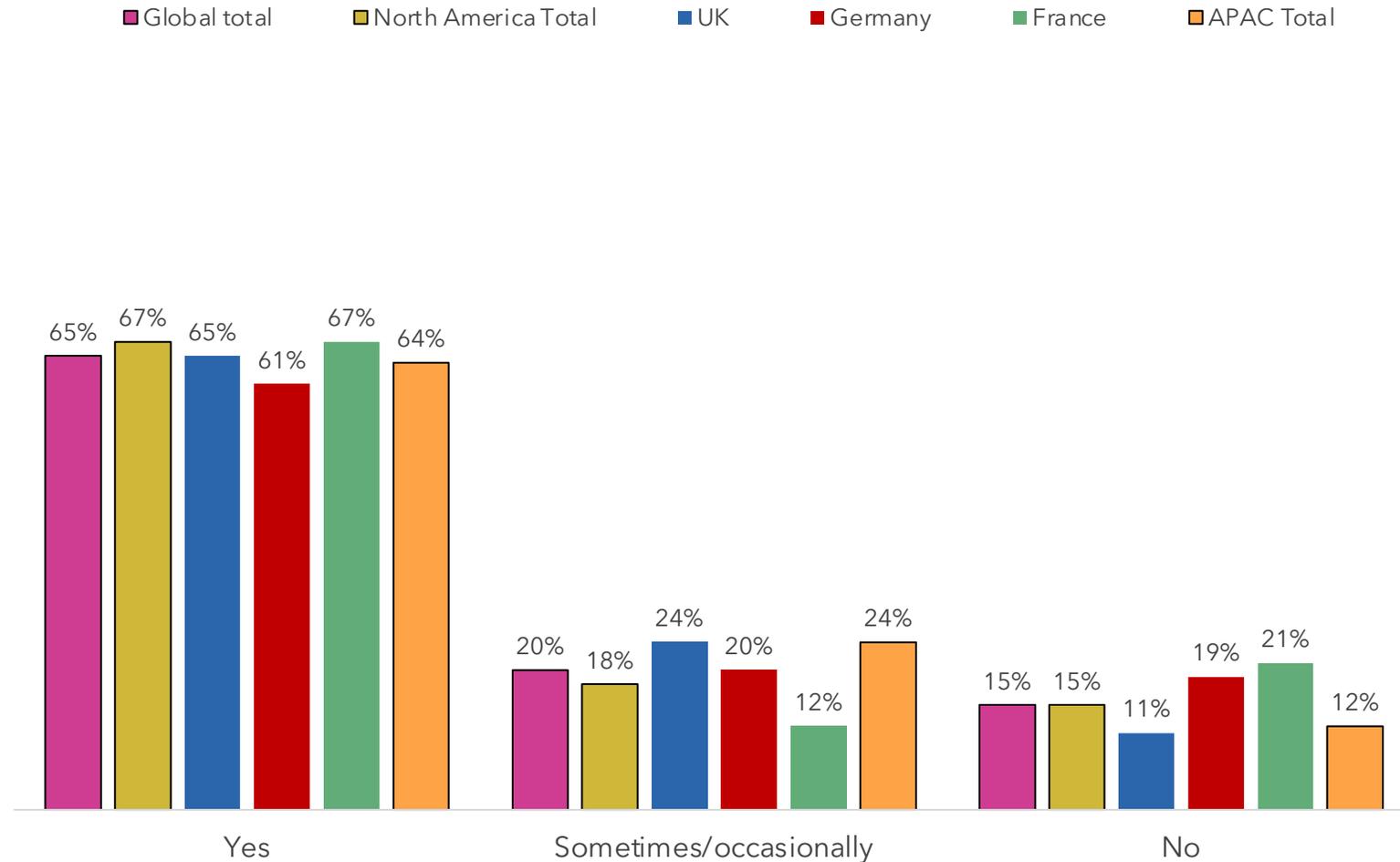
Base: Organizations that are required to adhere to the NIS2 Directive (525) North America (135) UK (171) Germany (64) France (87) APAC total (68)

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



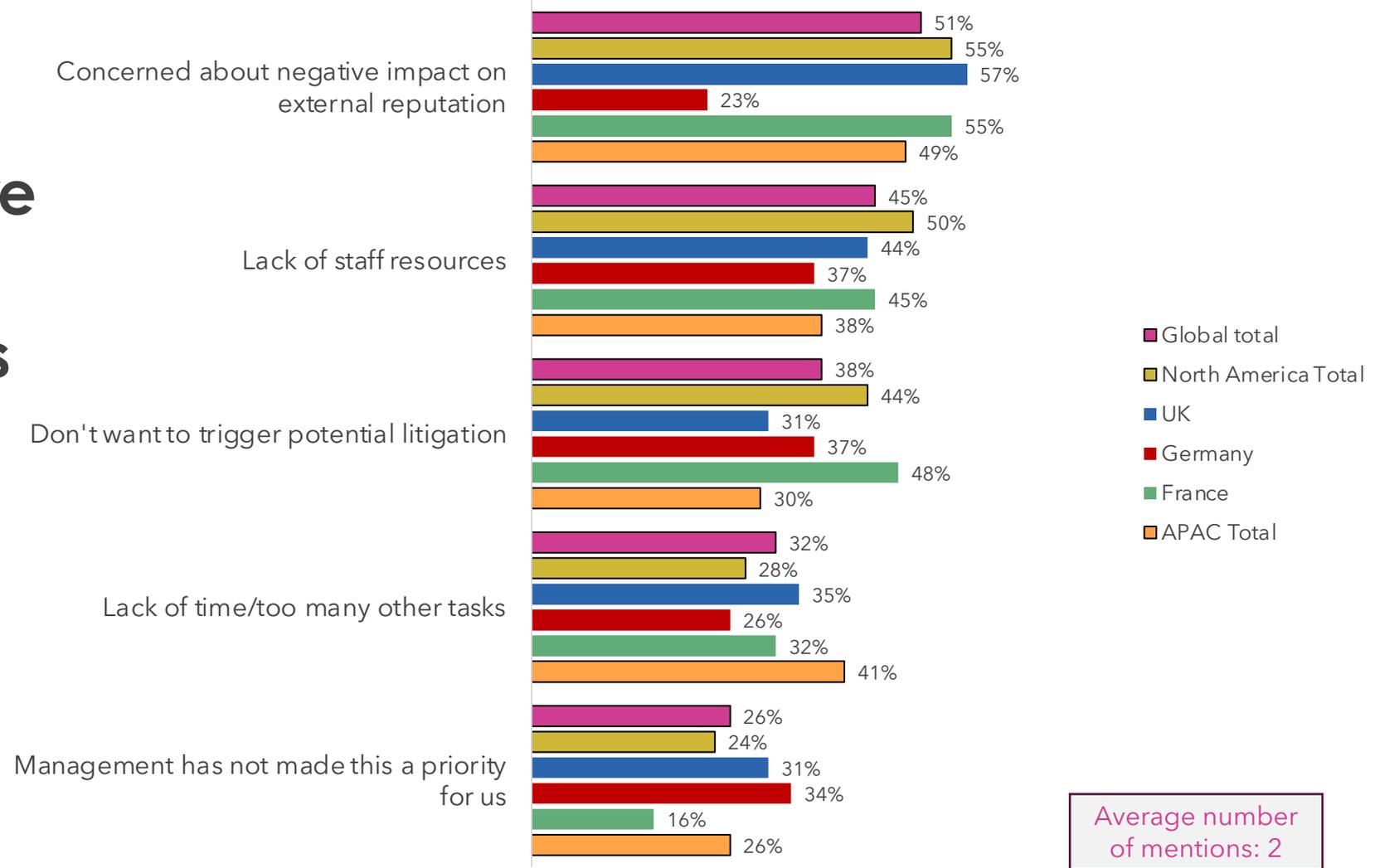
Base: Global total (1,000) North America (400) UK (200) Germany (100) France (100) APAC total (200)

Communicating vulnerabilities discovered in software produced to downstream consumers



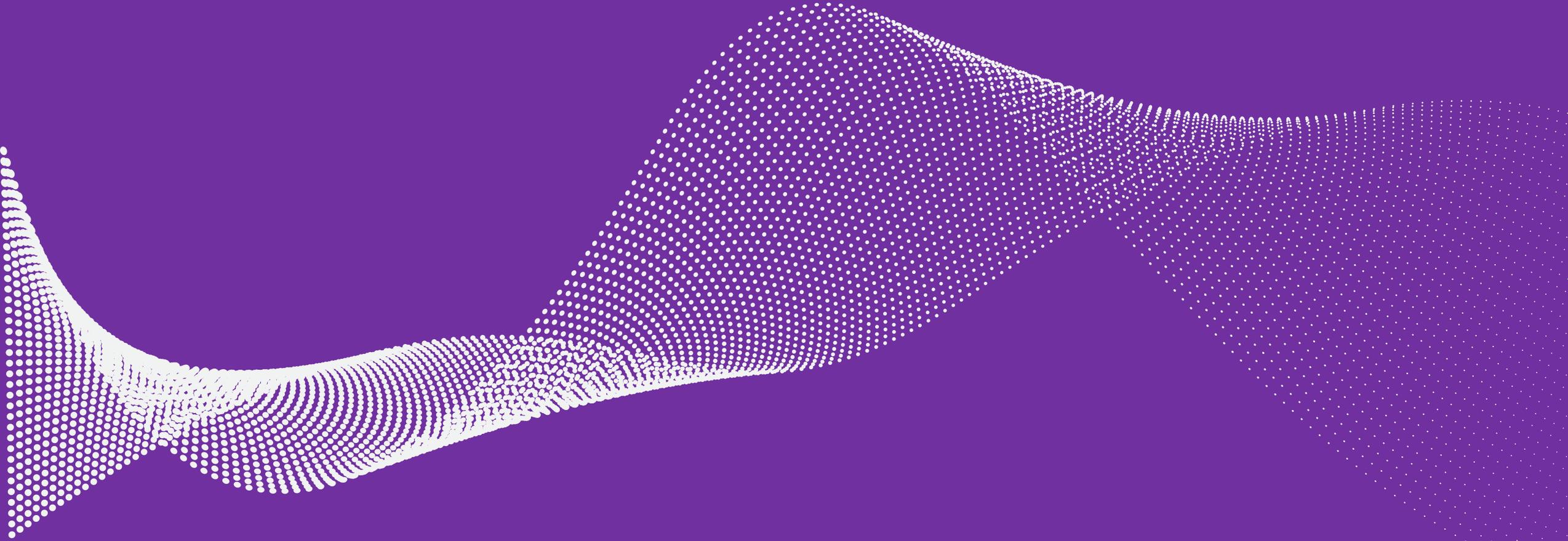
Base: All except those who don't produce software (959) North America (389) UK (192) Germany (91) France (94) APAC total (193)

Biggest obstacles to communicating software vulnerabilities to downstream consumers

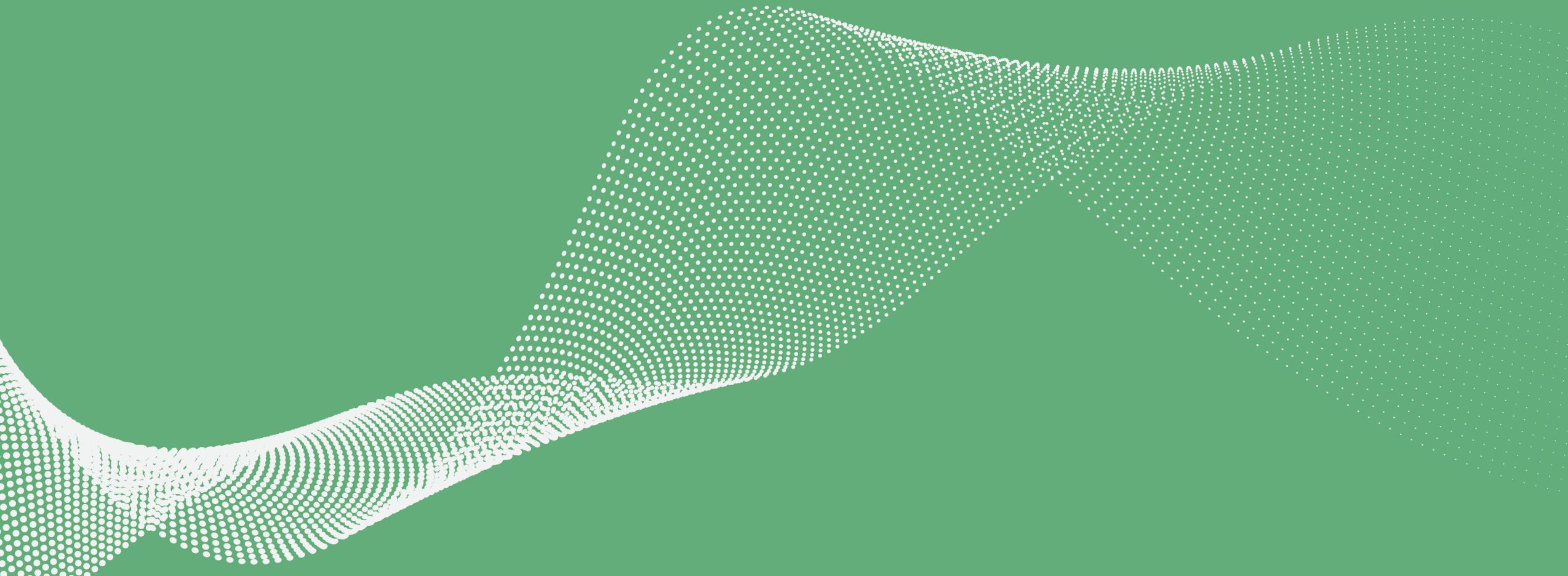


Base: Organisations where vulnerabilities are not communicated frequently (334) North America (131) UK (68) Germany (35) France (31) APAC total (69)

Thank you



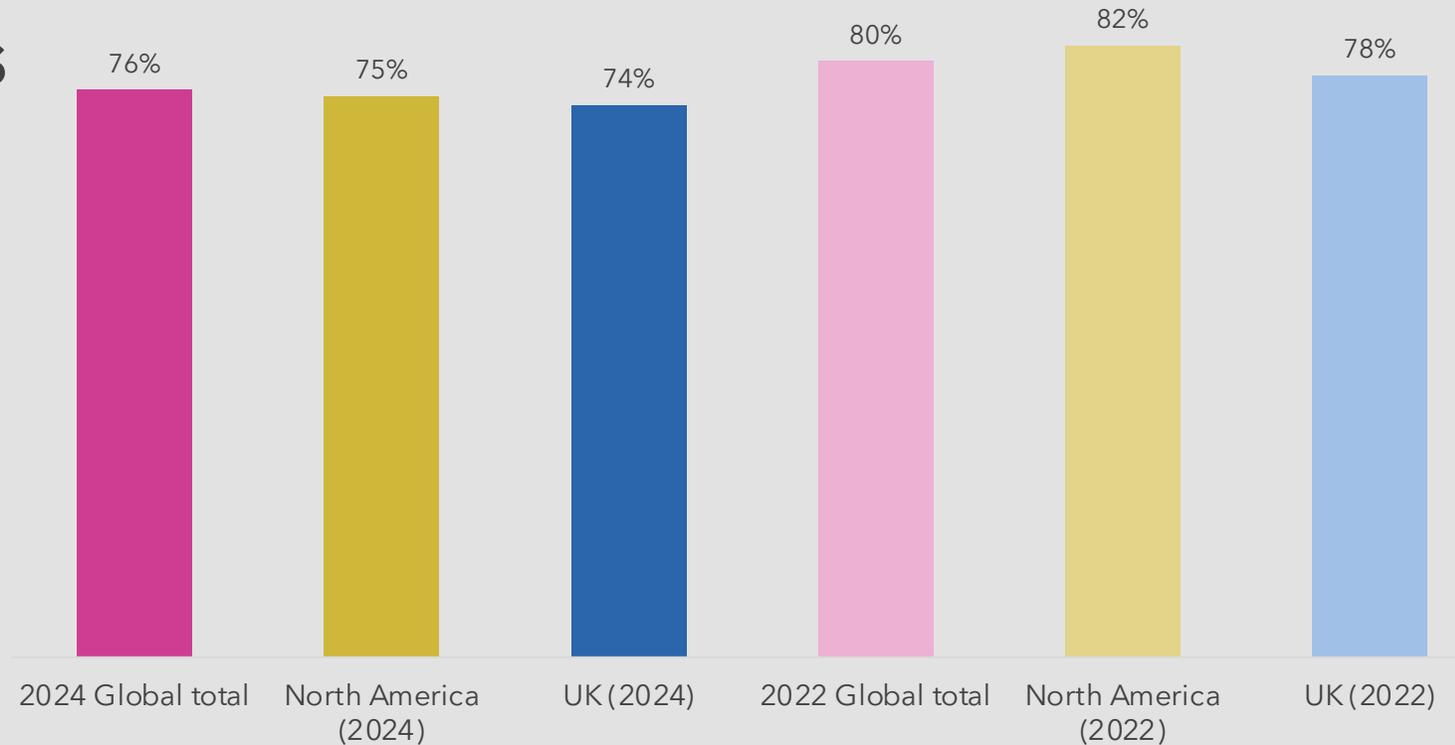
Appendix: 2022 vs 2024 comparison charts



2024 vs 2022 comparison

Yes responses

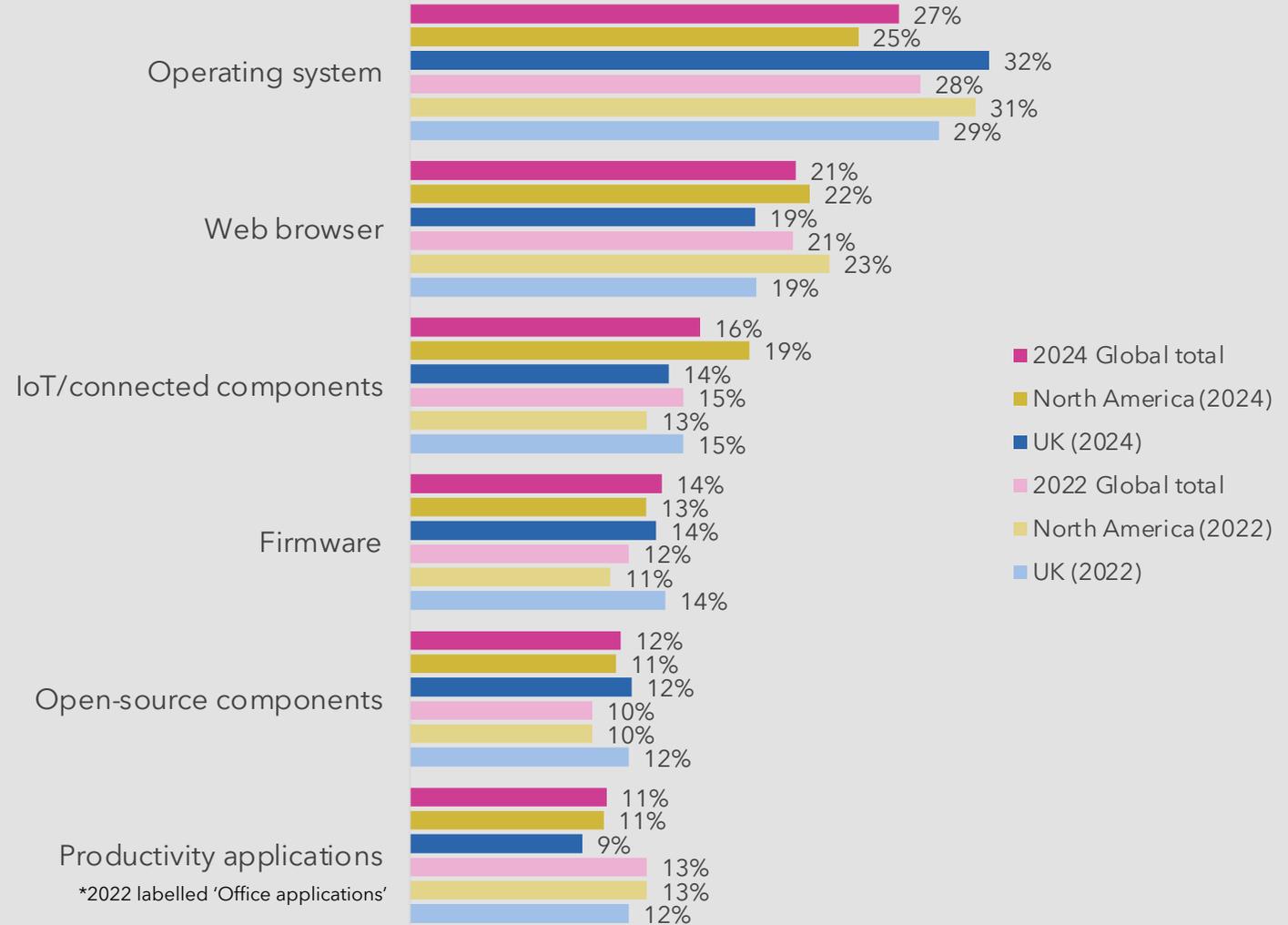
Being notified of a vulnerability or attack within software supply chain in last 12 months



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

2024 vs 2022 comparison

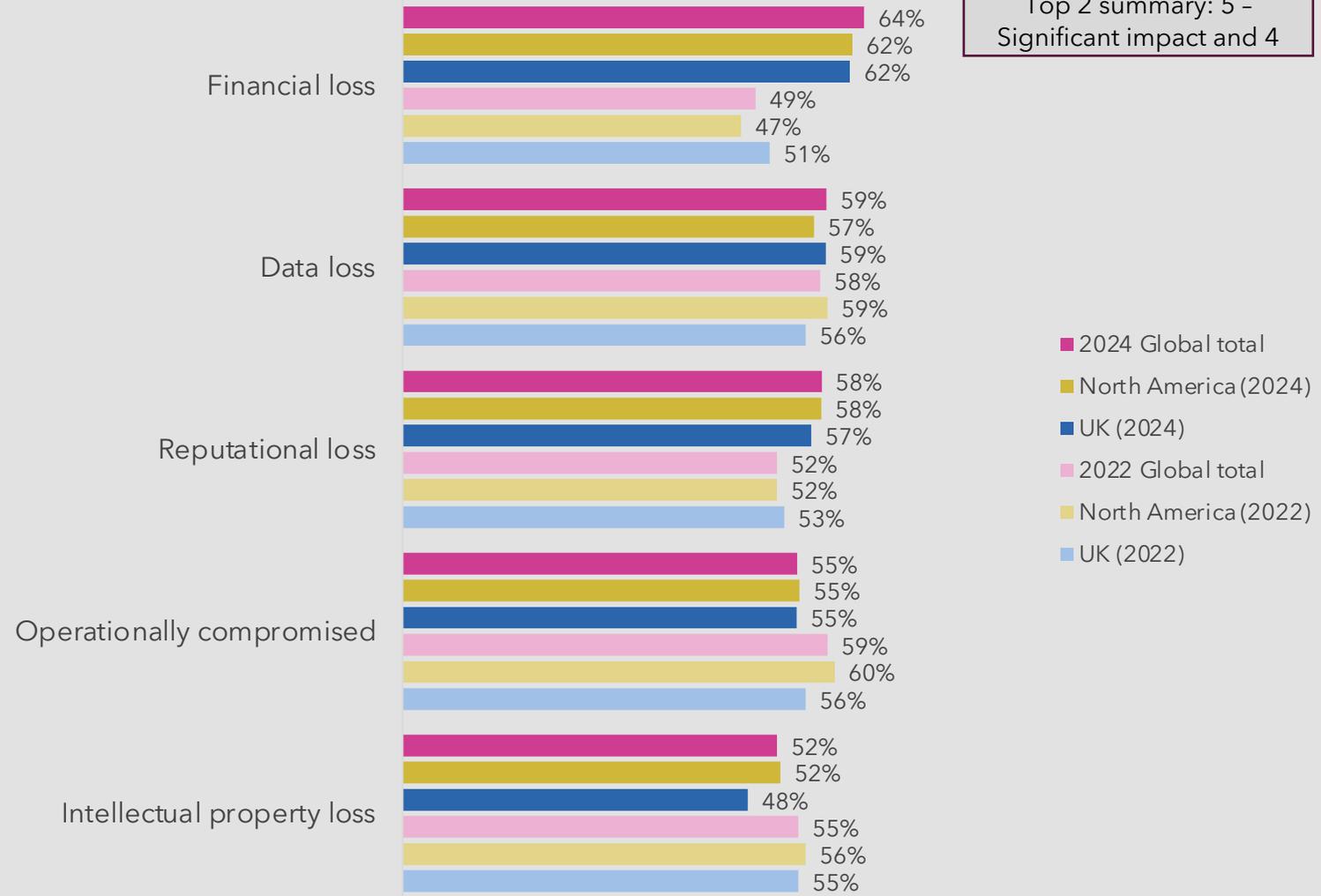
Vulnerable components having the biggest impact for organization



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)

2024 vs 2022 comparison

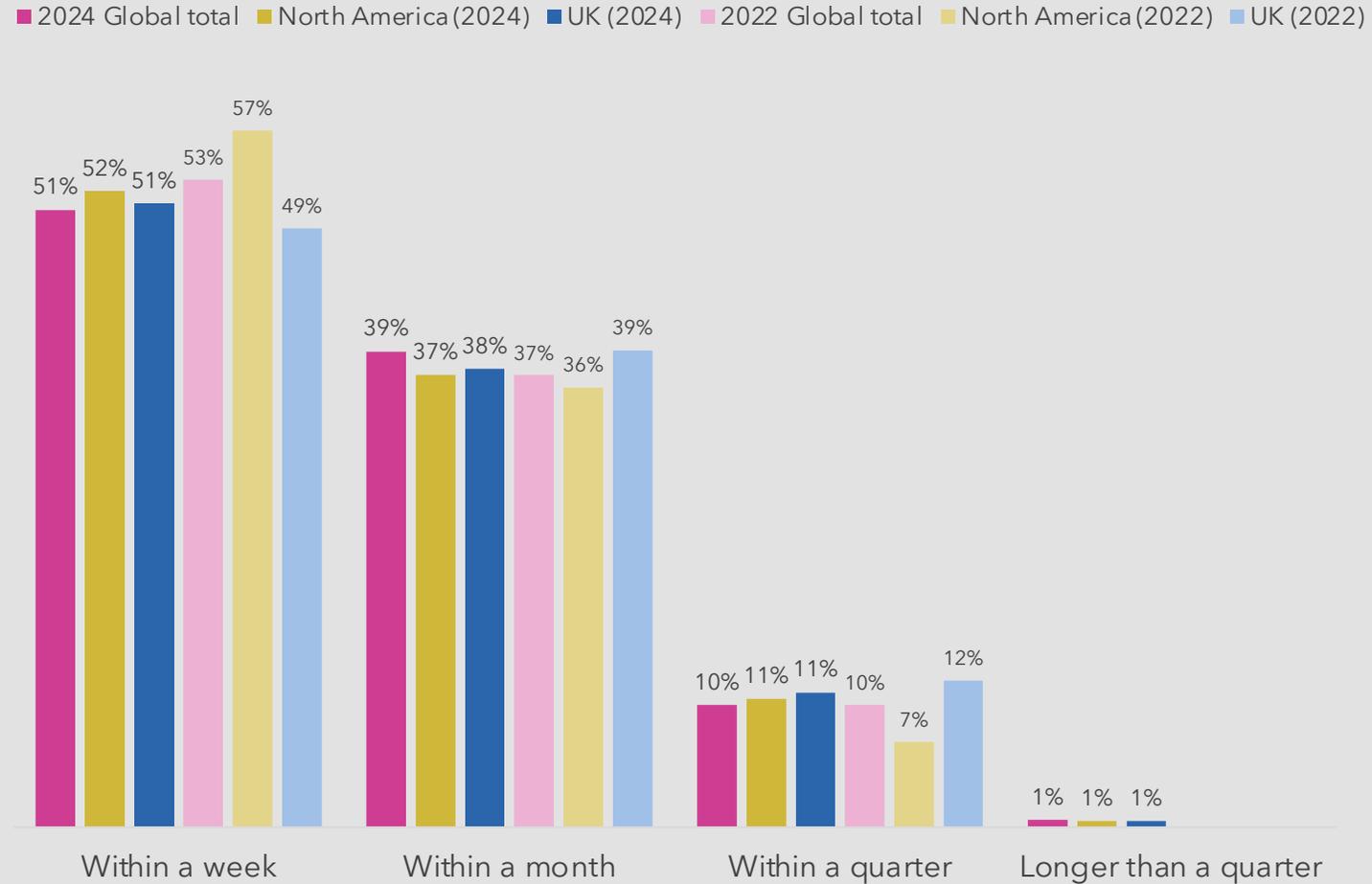
Significance of the attack on the business



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)

2024 vs 2022 comparison

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

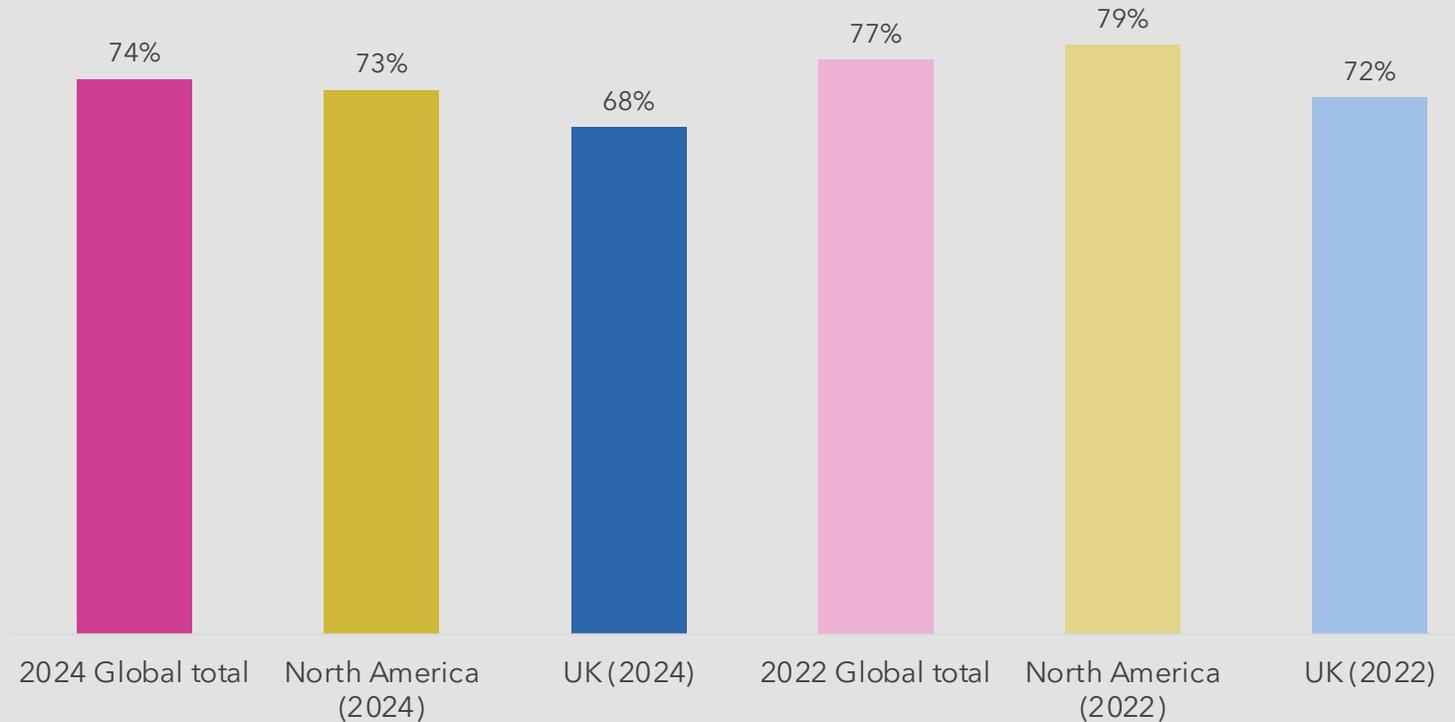


Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

2024 vs 2022 comparison

Yes responses

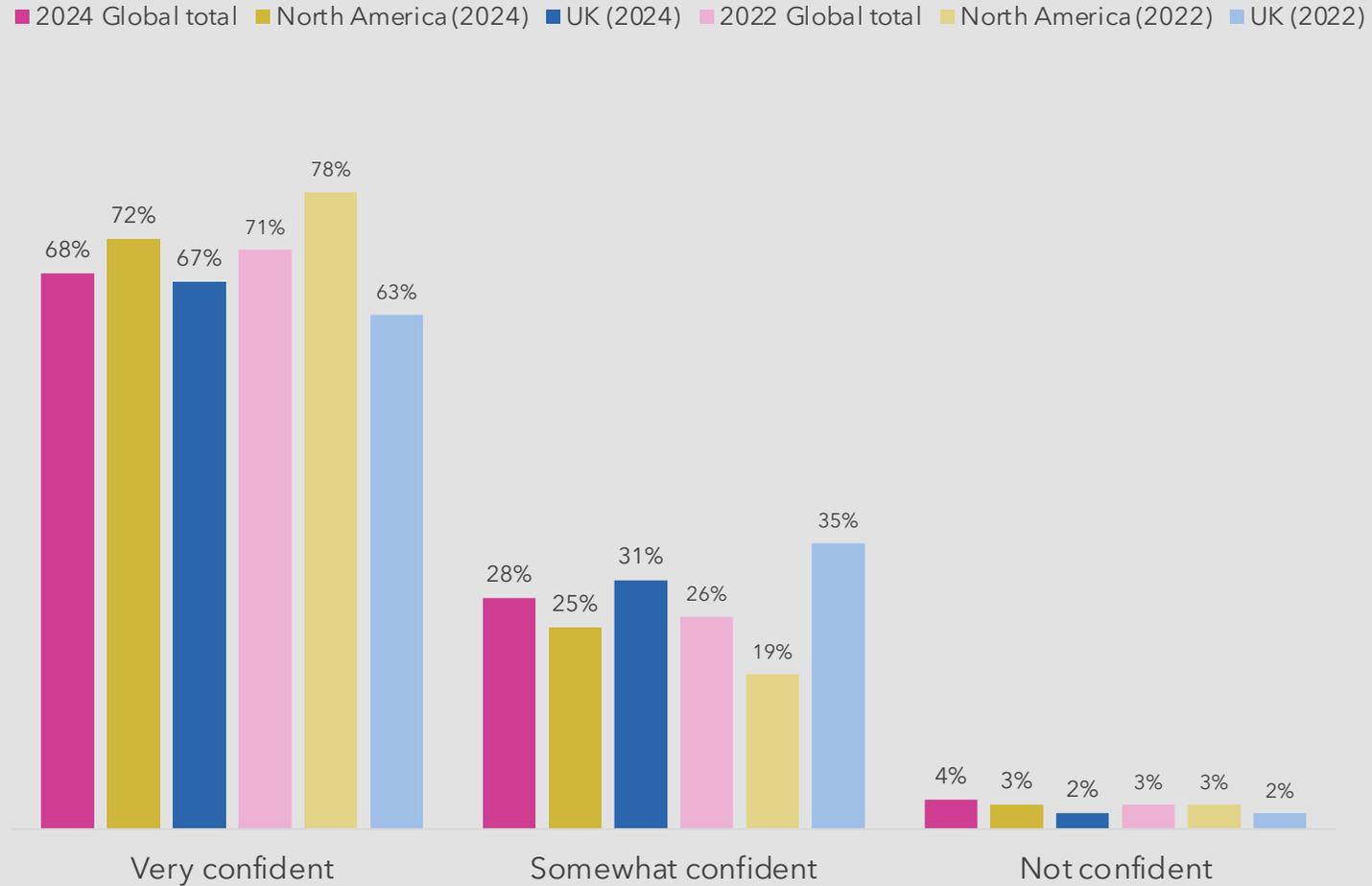
Made aware of a member of supply chain not previously aware of / monitoring for security practices



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

2024 vs 2022 comparison

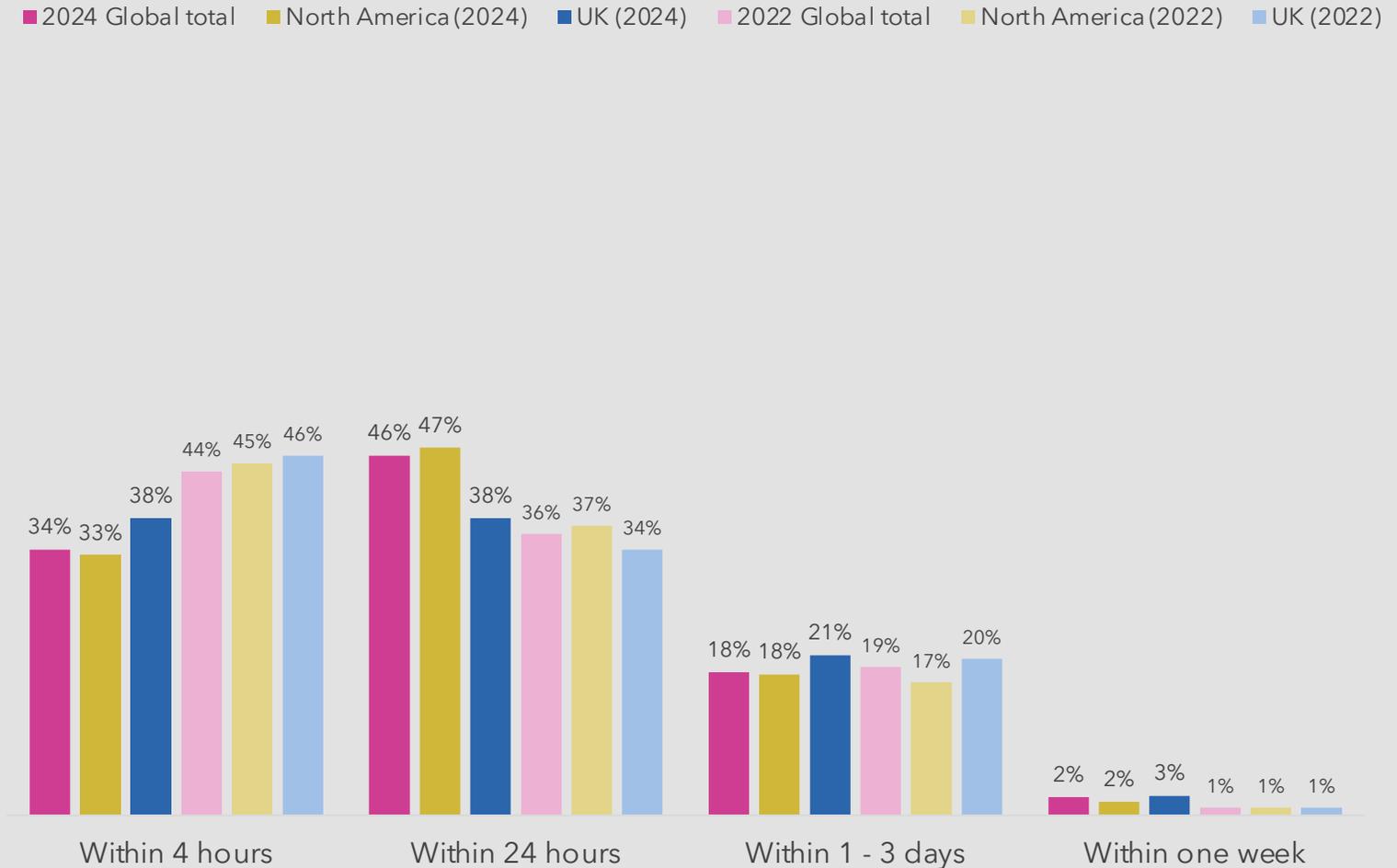
Confidence that suppliers / partners can identify and prevent a vulnerability



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

2024 vs 2022 comparison

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

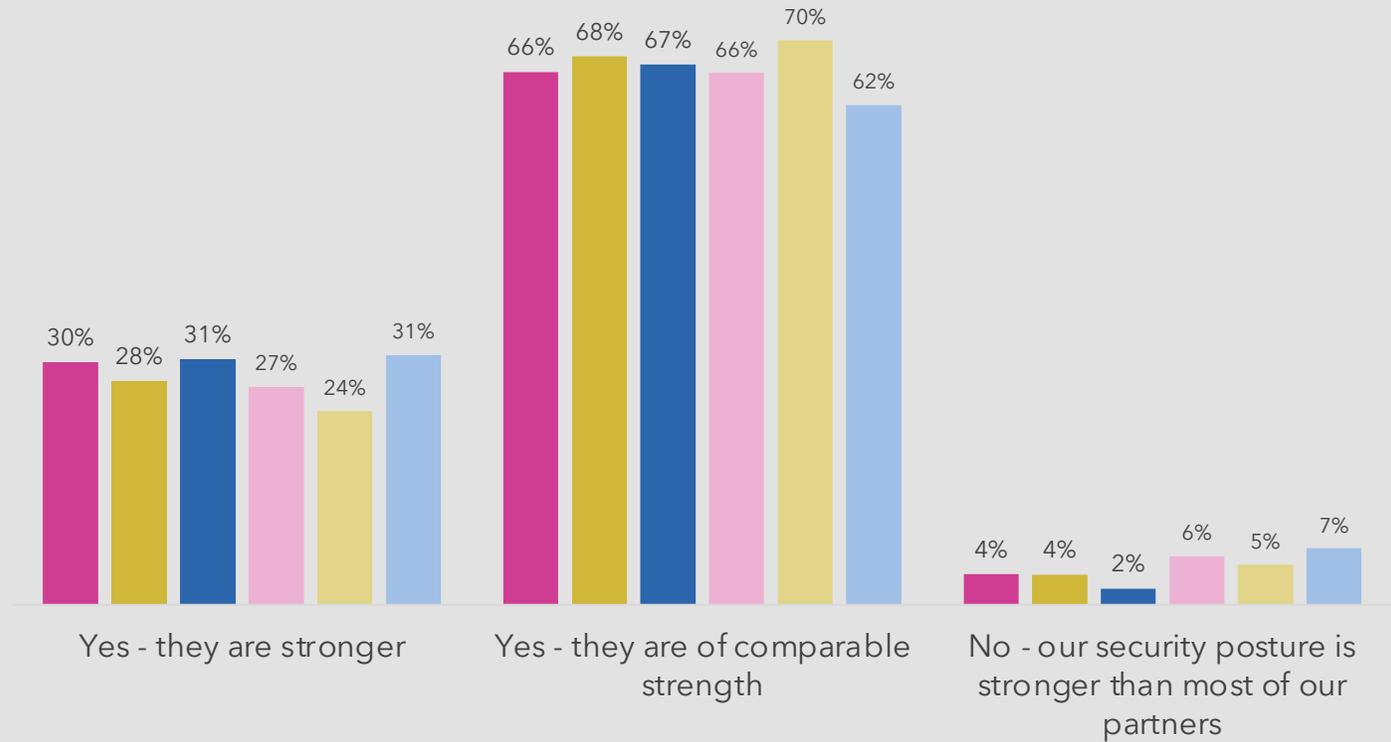


Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

2024 vs 2022 comparison

Comparability of suppliers / partners cybersecurity policies

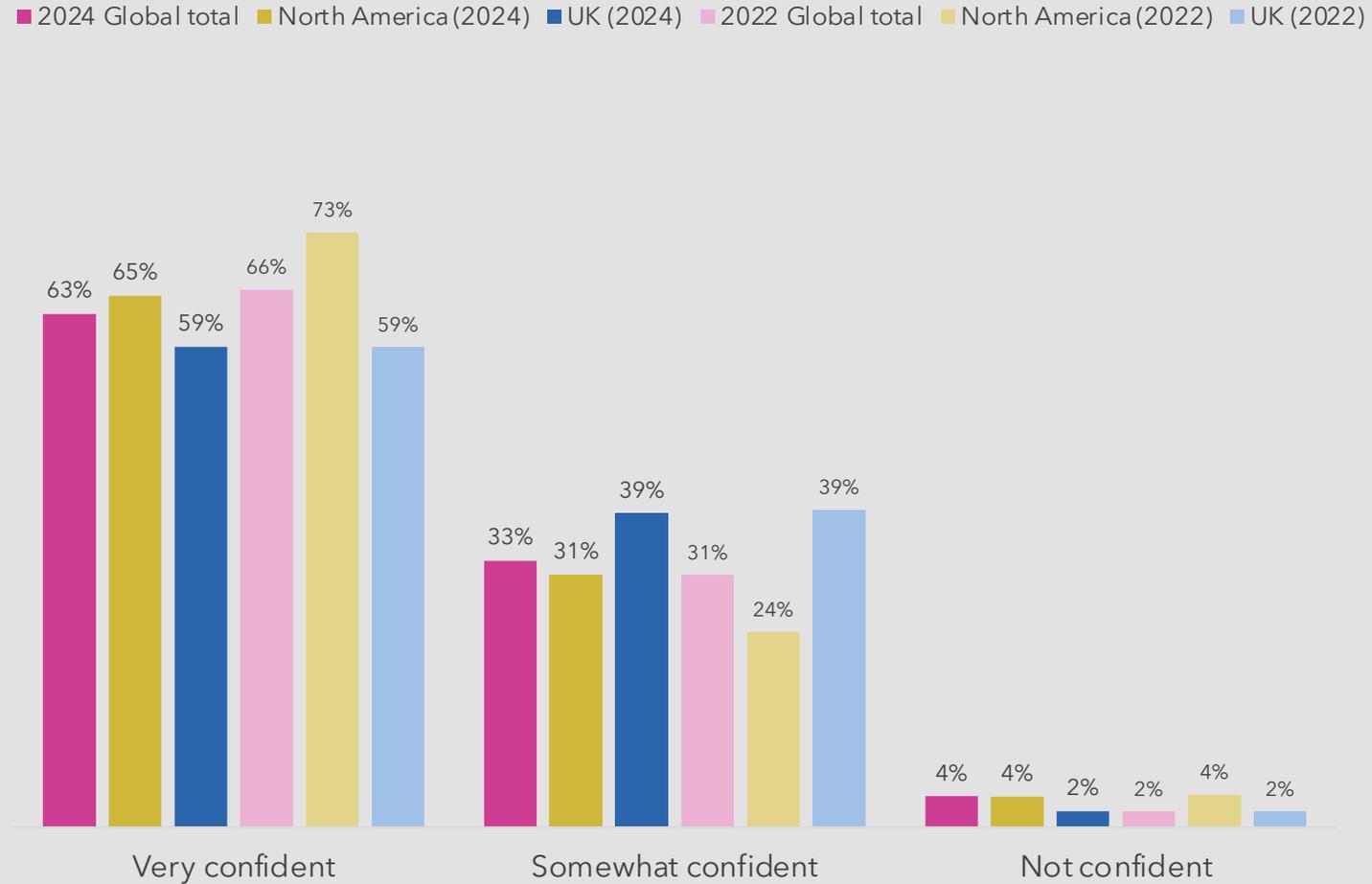
■ 2024 Global total ■ North America (2024) ■ UK (2024) ■ 2022 Global total ■ North America (2022) ■ UK (2022)



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

2024 vs 2022 comparison

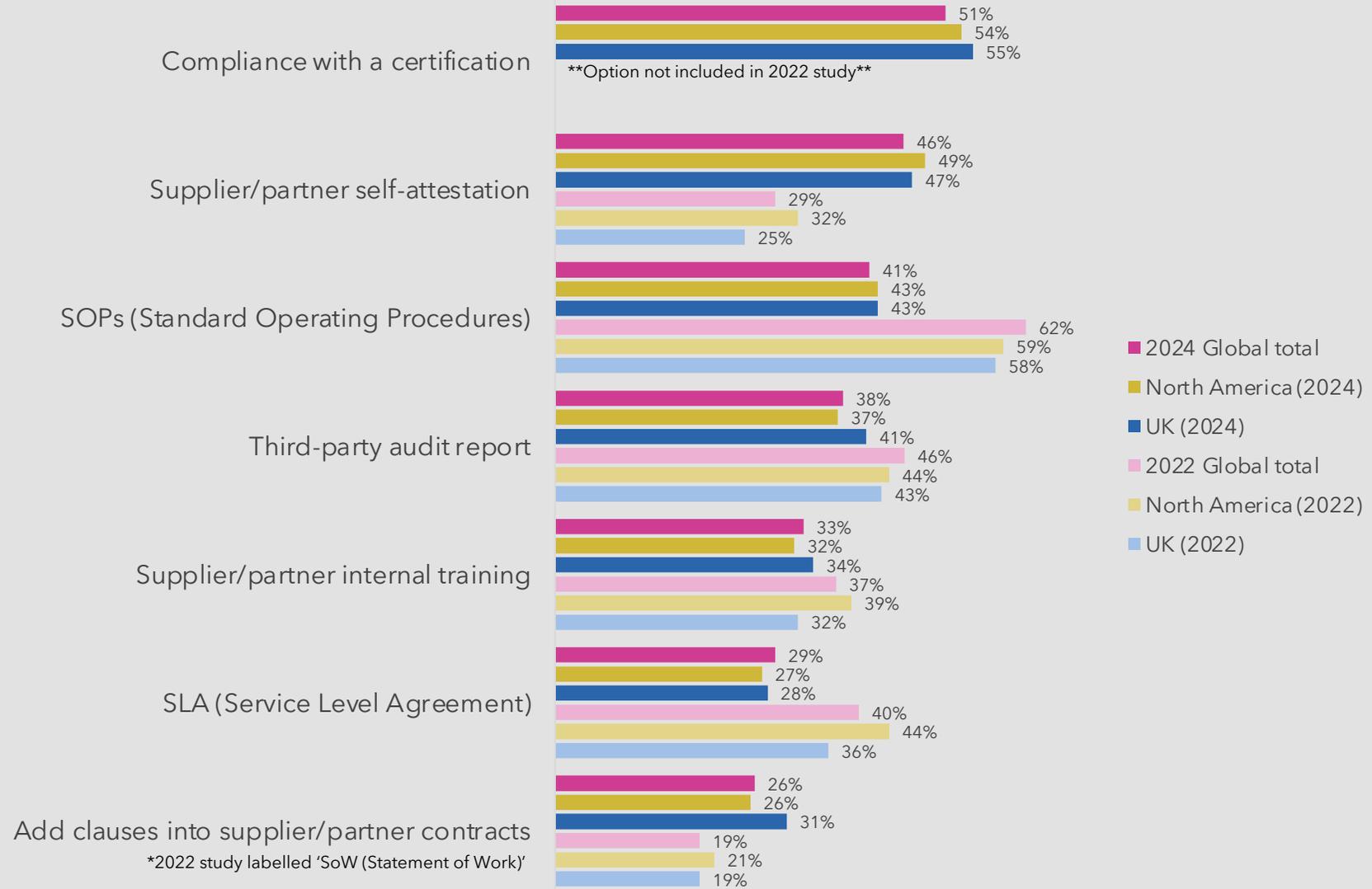
Confidence that suppliers / supply chain partners have adequate cybersecurity regulatory and compliance practice



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

2024 vs 2022 comparison

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

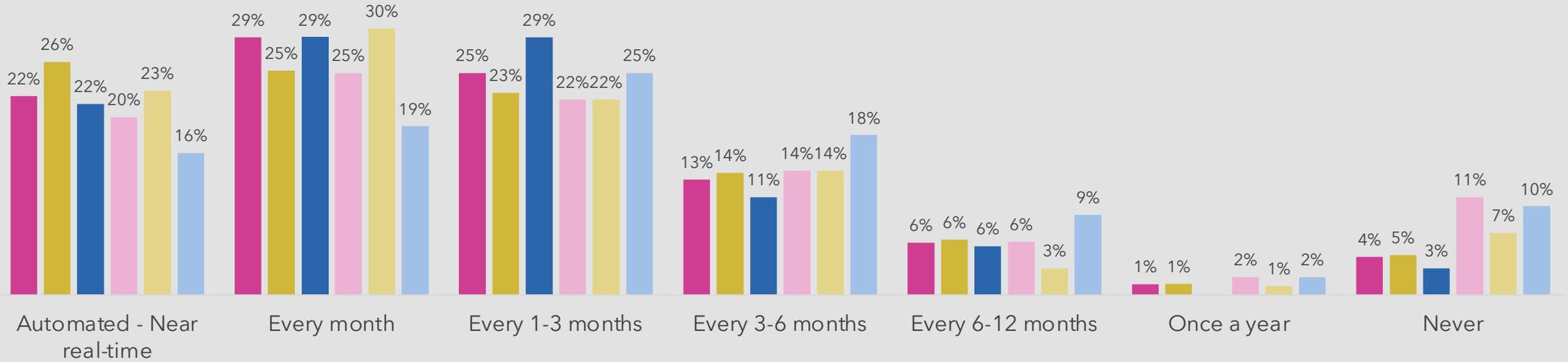


Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

2024 vs 2022 comparison

■ 2024 Global total ■ North America (2024) ■ UK (2024) ■ 2022 Global total ■ North America (2022) ■ UK (2022)

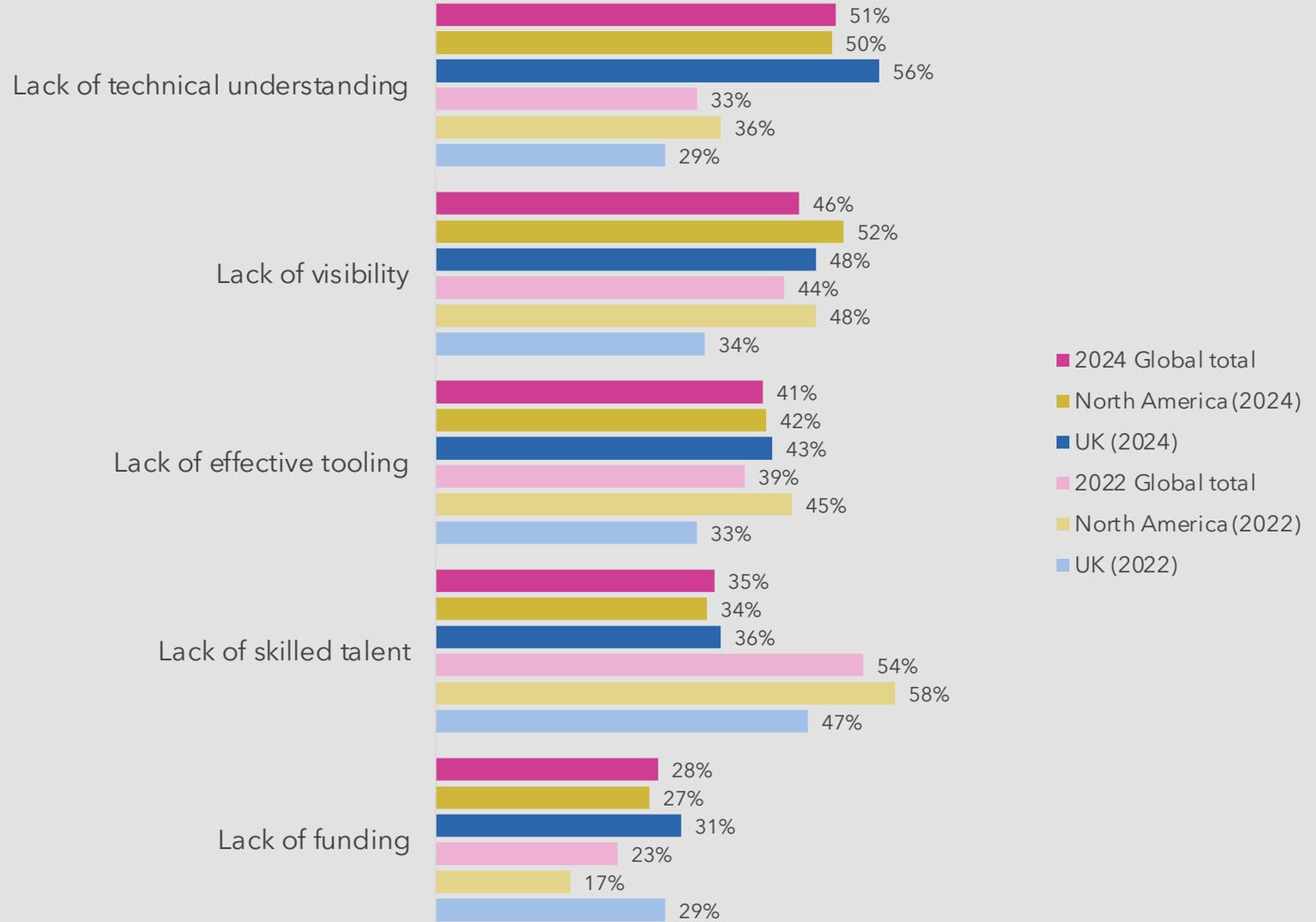
Frequency of performing inventories of own software environment



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

2024 vs 2022 comparison

Biggest barriers to regular software inventories

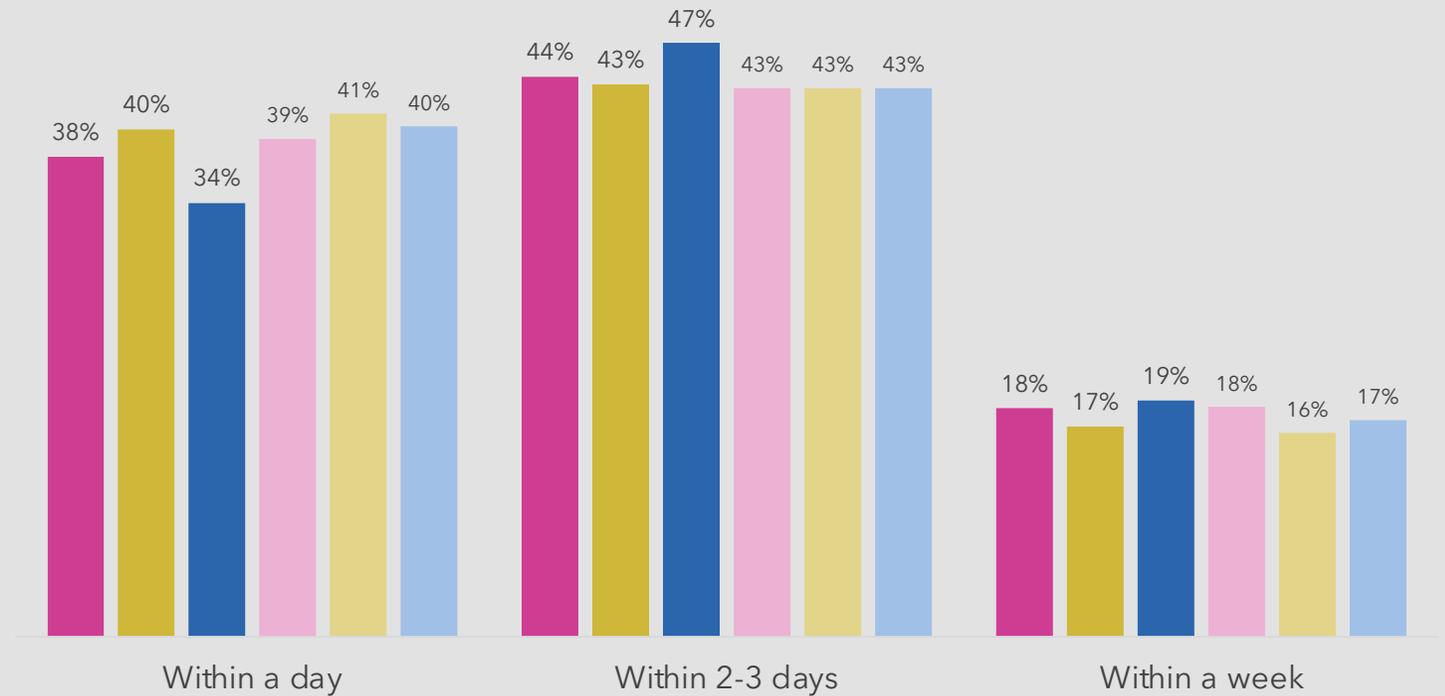


Base: Global total <2024> (1,000) North America (400) UK (200) <2022> (1,500) North America (500) UK (500)

2024 vs 2022 comparison

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

■ 2024 Global total ■ North America (2024) ■ UK (2024) ■ 2022 Global total ■ North America (2022) ■ UK (2022)



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

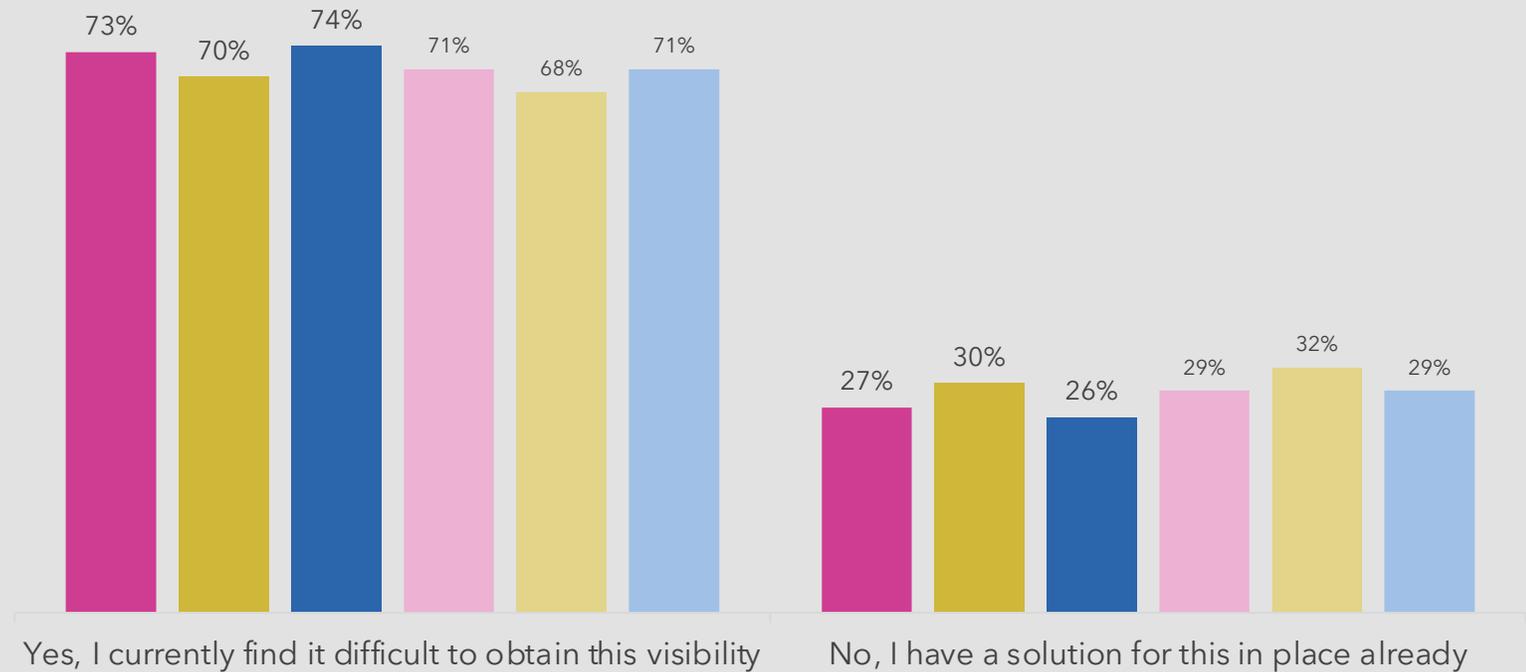
Single coded question

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

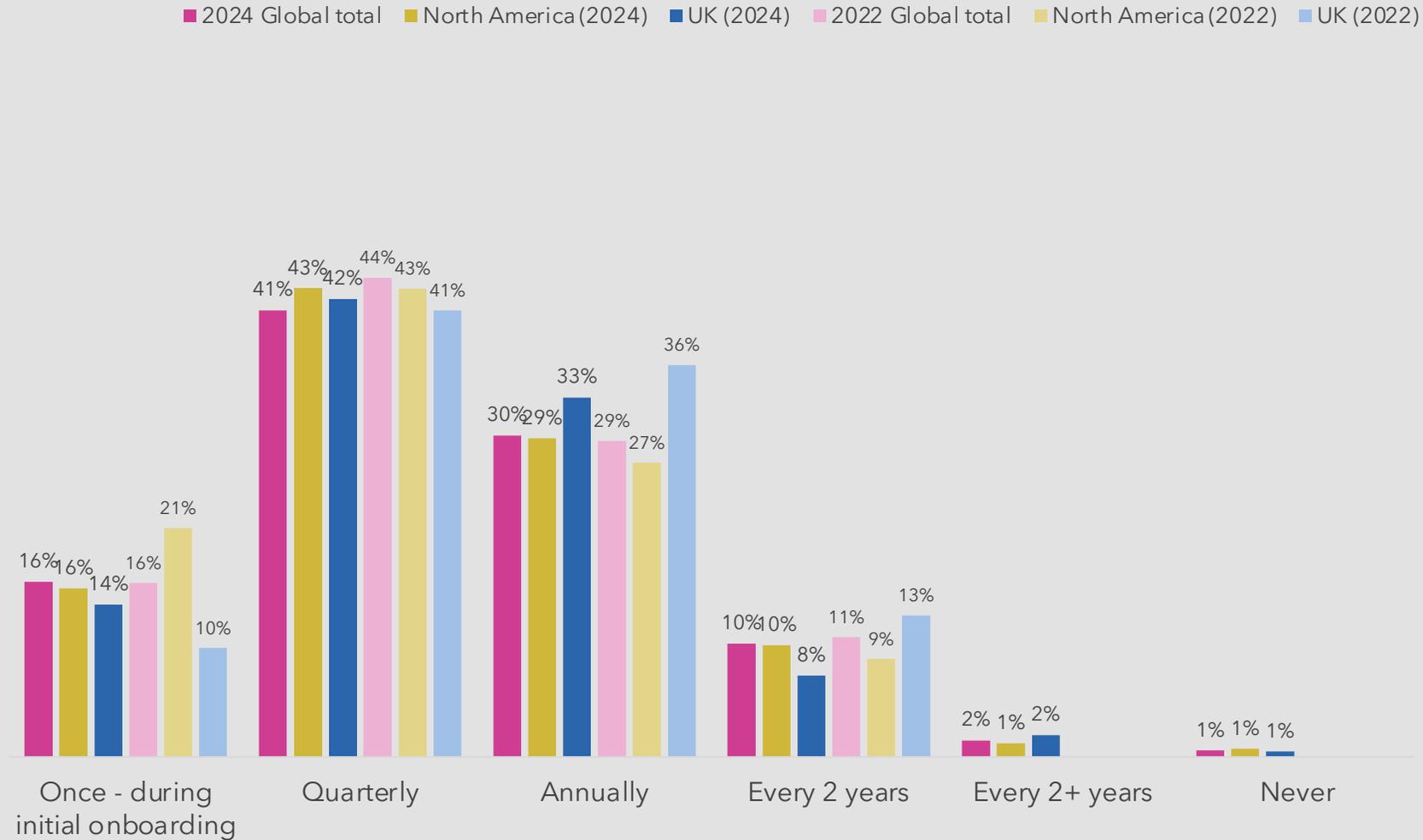
■ 2024 Global total ■ North America (2024) ■ UK (2024) ■ 2022 Global total ■ North America (2022) ■ UK (2022)



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

2024 vs 2022 comparison

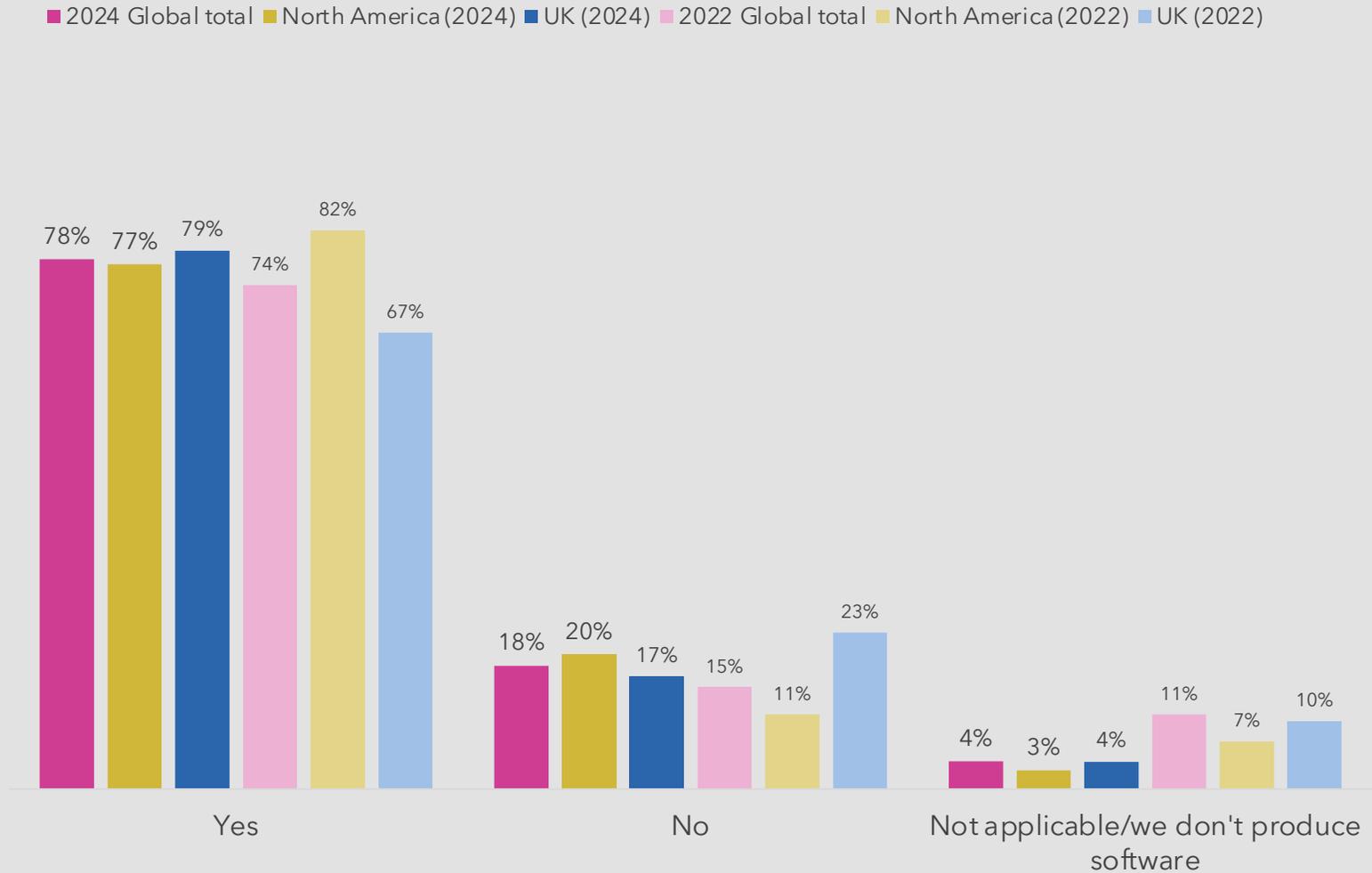
Frequency of suppliers/ partners to provide evidence of compliance to security certifications and frameworks



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

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)