Securing the supply chain

CrowdStrike
Research results

June 2018

VansonBourne

Demographics - respondents

1,300 senior IT decision makers and IT security professionals were interviewed in April and May 2018 split in the following ways...

…respondent country

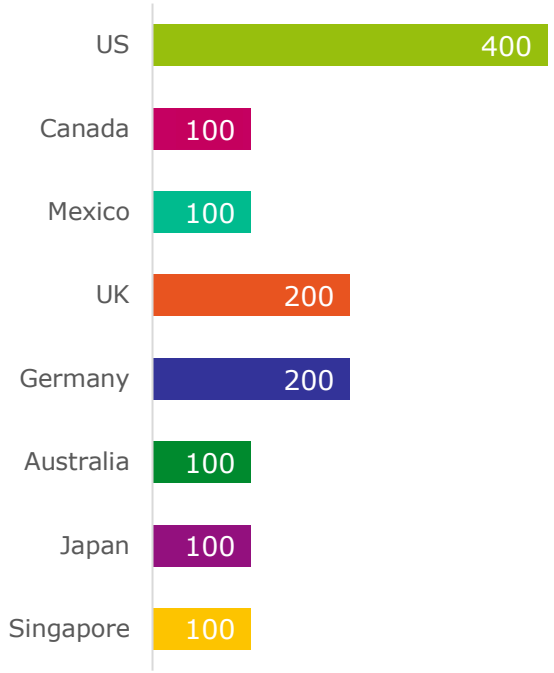


Figure D1: *Analysis of respondents' country. Asked to all respondents (1,300)*

…respondent type

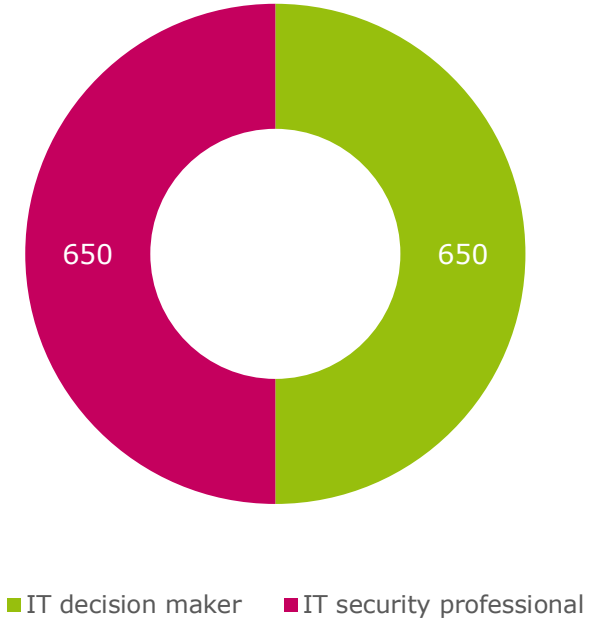


Figure D2: *Analysis of respondent type. Asked to all respondents (1,300)*

…respondent job role

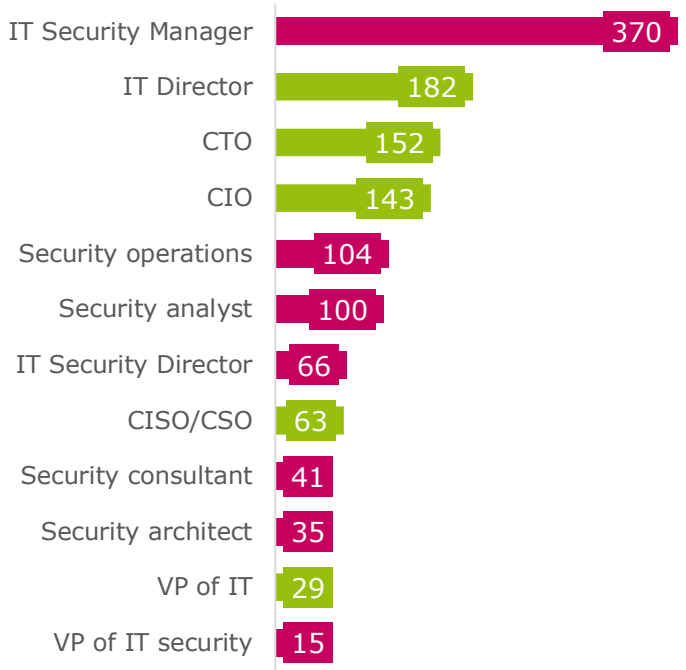


Figure D3: "Which of the following best describes your job role in your organization?" *asked to all respondents (1,300)*

VansonBourne

Demographics – respondents' organizations

1,300 senior IT decision makers and IT security professionals were interviewed in April and May 2018 split in the following ways...

…organization sector

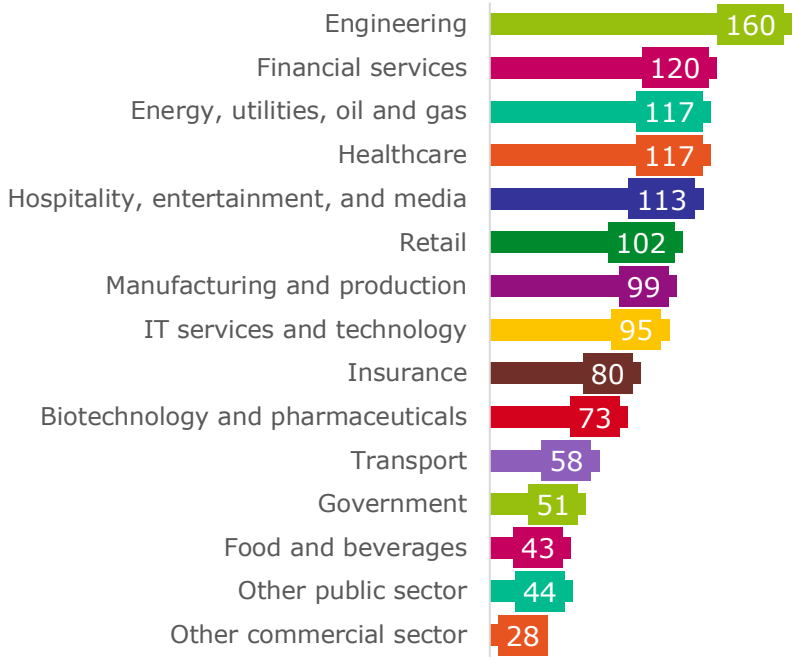


Figure D4: "Within which sector is your organization?" *asked to all respondents (1,300)*

…organization size

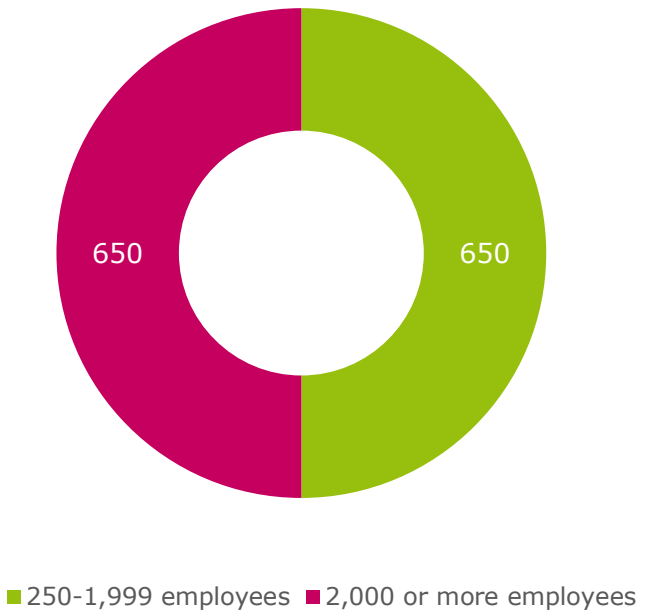


Figure D5: "How many employees does your organization have globally?" *asked to all respondents (1,300)*

…organization's total annual IT/cyber security spend

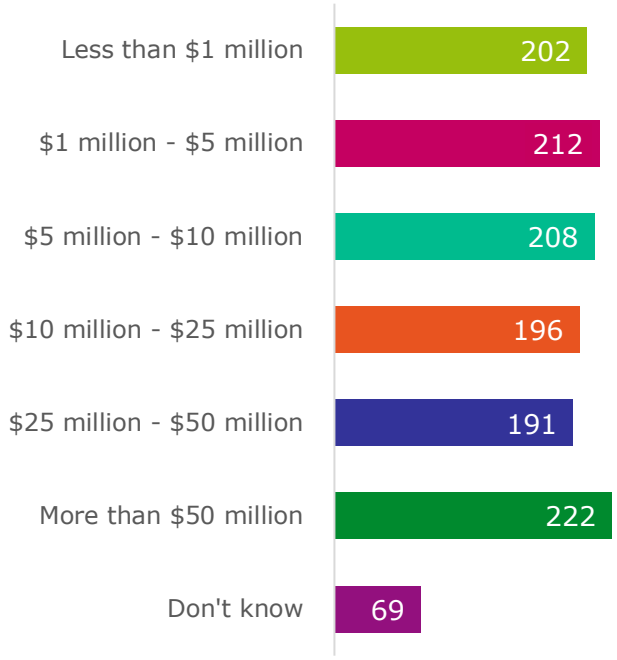


Figure D6: "What is your organization's total annual spend on IT/cyber security?" *asked to all respondents (1,300)*

VansonBourne

Four areas of interest:

1: The cyber security conundrum
2: The security disruptor – supply chain attacks
3: Eliminating the weakest link
4: When the chain breaks

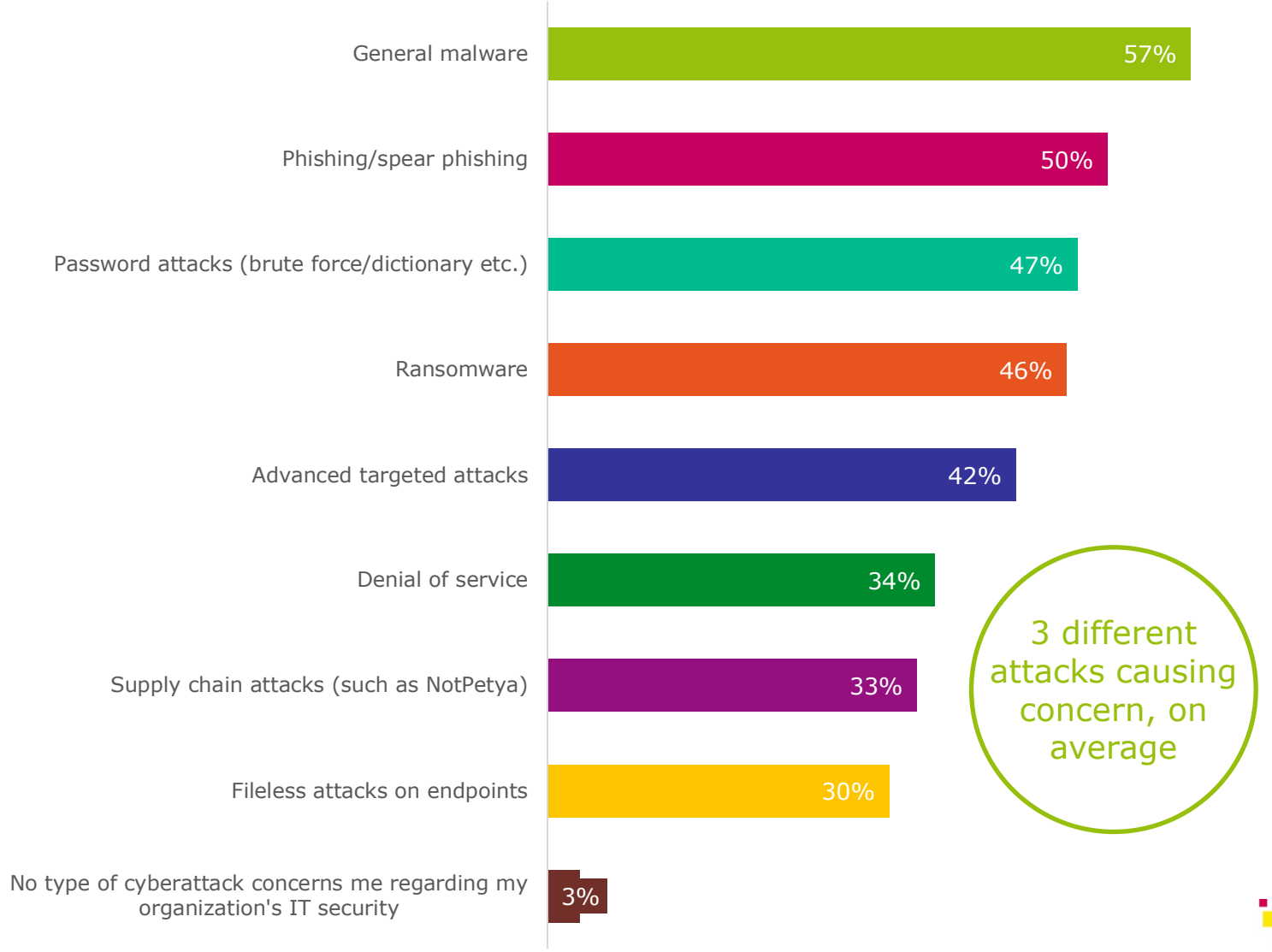
VansonBourne

1: The cyber security conundrum

VansonBourne

Overall cyber security concerns

Nearly all (97%) respondents recognize at least one type of cyberattack that causes concern for their organization for the next 12 months



3 different attacks causing concern, on average

Figure 1: "Thinking about your organization's IT security over the next 12 months, which of the following types of cyberattack are causing concern in your organization?" *asked to all respondents (1,300)*

VansonBourne

Different respondents with different concerns…

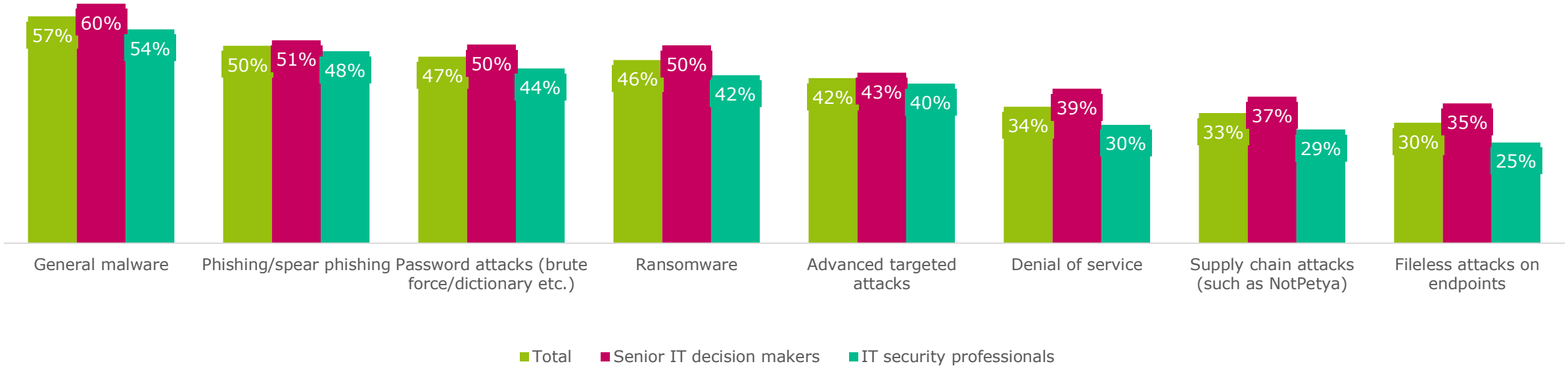
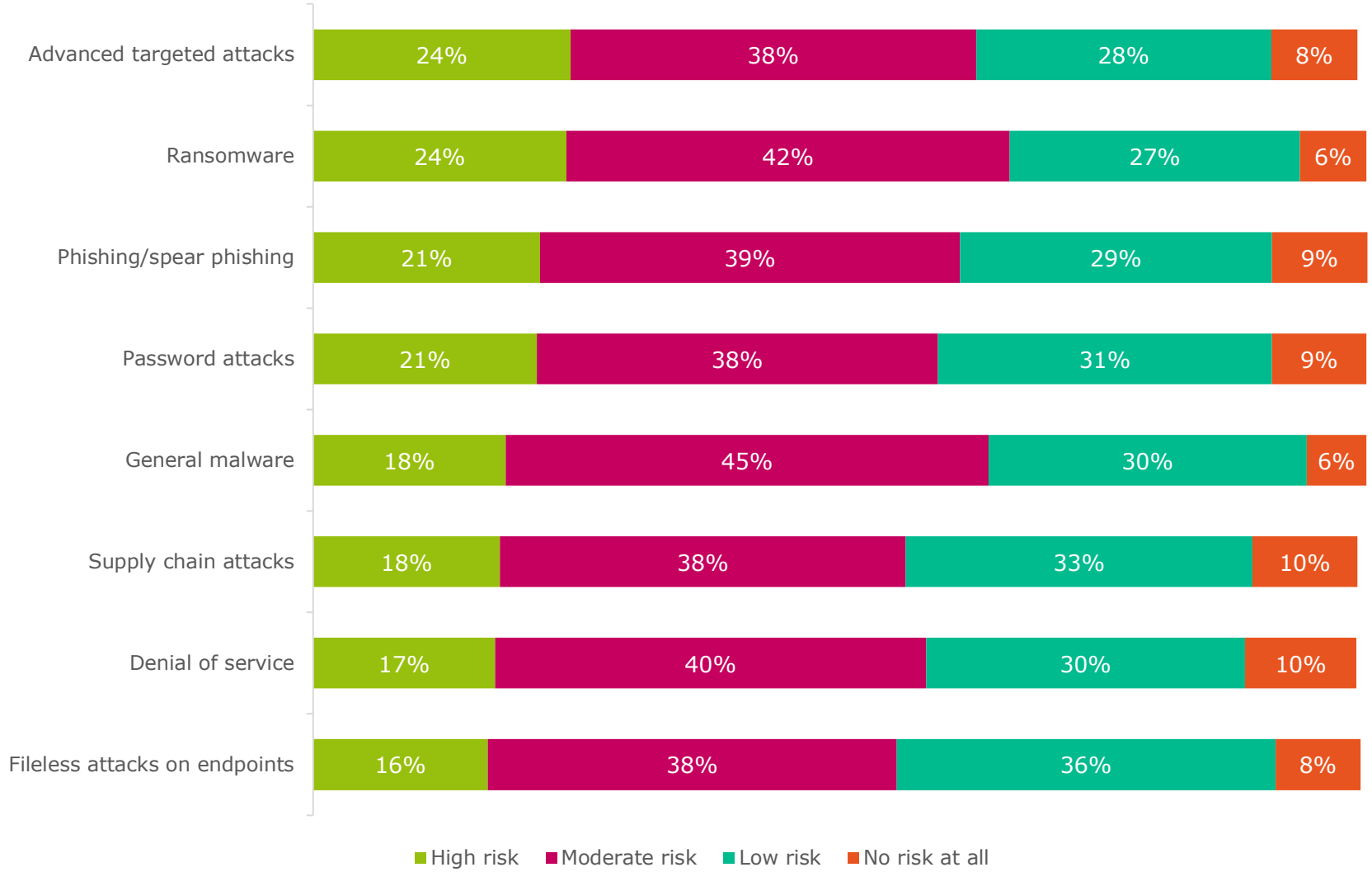


Figure 2: "Thinking about your organization's IT security over the next 12 months, which of the following types of cyberattack are causing concern in your organization?" *asked to all respondents, split by respondent type (1,300)*

VansonBourne

Risk posed by cyberattack



Only a minority (10-6%) of respondents feel that they are at no risk from the listed cyberattacks

Figure 3: "How would you define the level of risk that you feel that your organization is currently exposed to regarding the following cyberattacks?" *asked to all respondents, but excluding 'don't know' responses (1,300)*

VansonBourne

Preparing to defend against attack

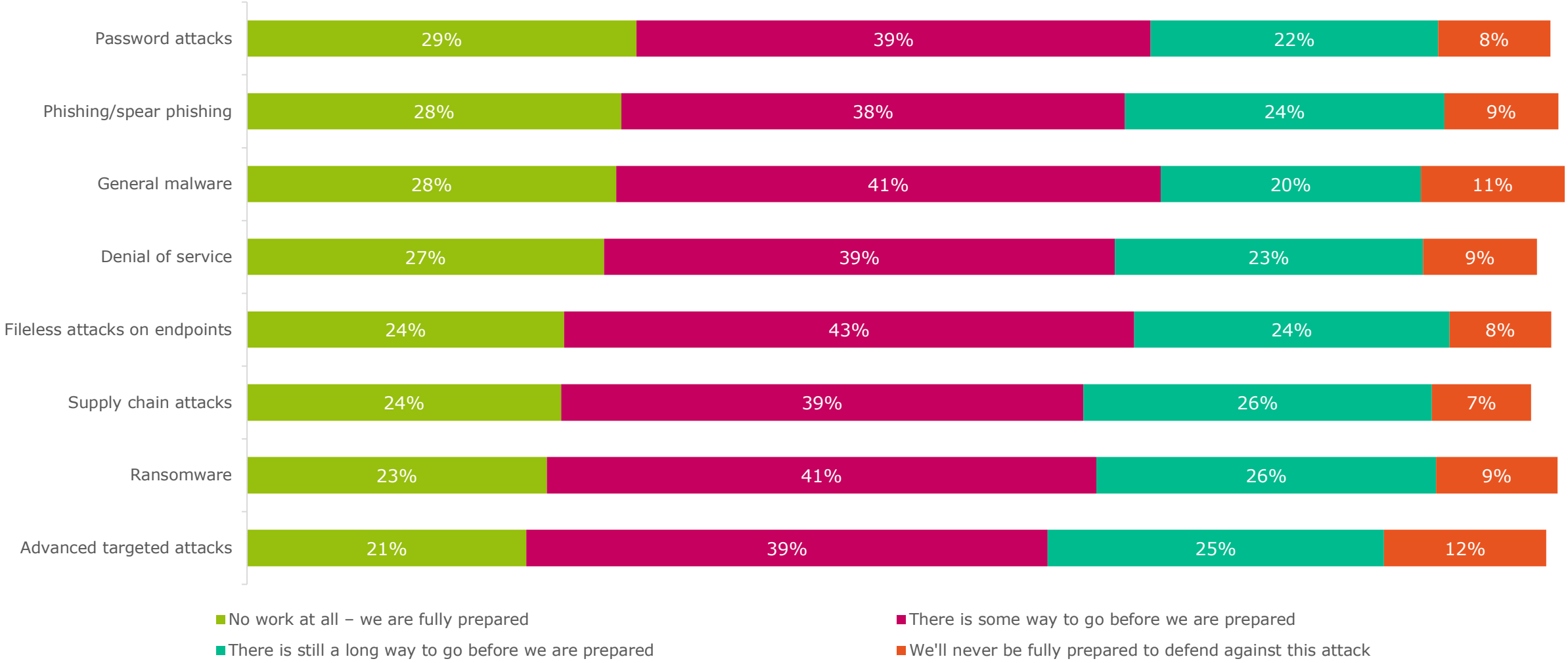


Figure 4: "How much work does your organization still need to do in order to be fully prepared to defend against each of the following attacks?" *asked to all respondents, but excluding 'don't know' responses (1,300)*

VansonBourne

Behind the cyberattack

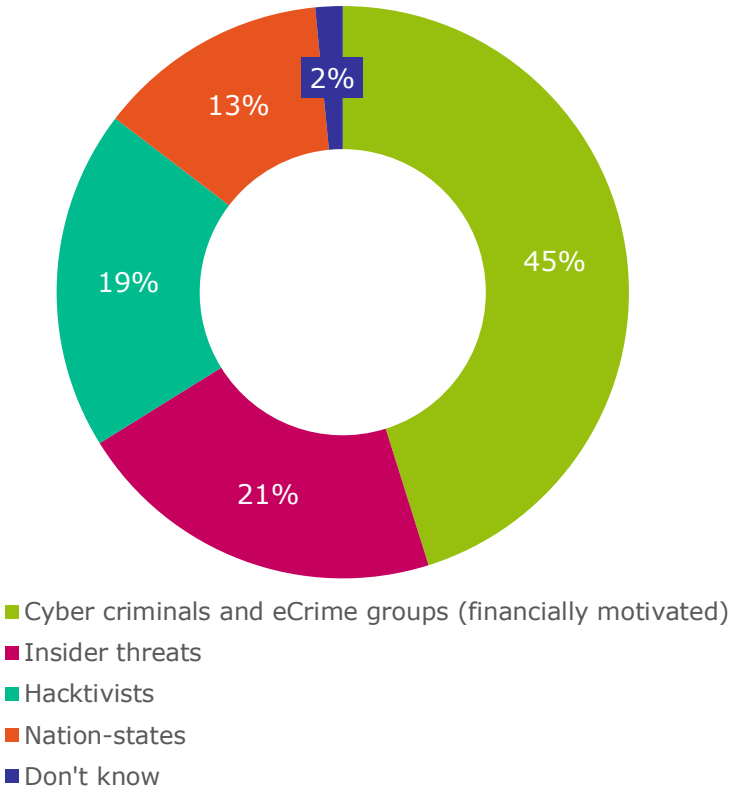


Figure 5: "Thinking of all of the different types of cyber attacker who may target your organization, which concerns your organization the most?" *asked to all respondents (1,300)*

Cyberattacks from organized cyber criminals and eCrime groups worry approaching half of respondents the most (45%)

Regardless of who the attacker is, the vast majority (88%) see it as either crucial or important that they find out who is behind the attack

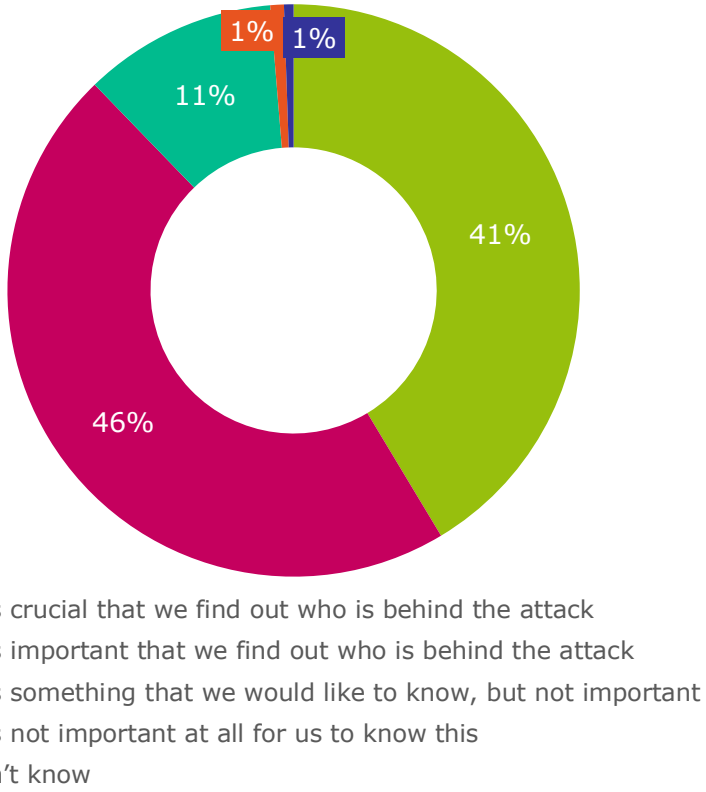


Figure 6: "How important is the attribution of cyberattacks to your organization's security strategy?" *asked to all respondents (1,300)*

VansonBourne

Attacks by nation-states

No nation is particularly concerned by nation-state cyberattacks, but respondents in Mexico show the lowest levels (4%) of concern

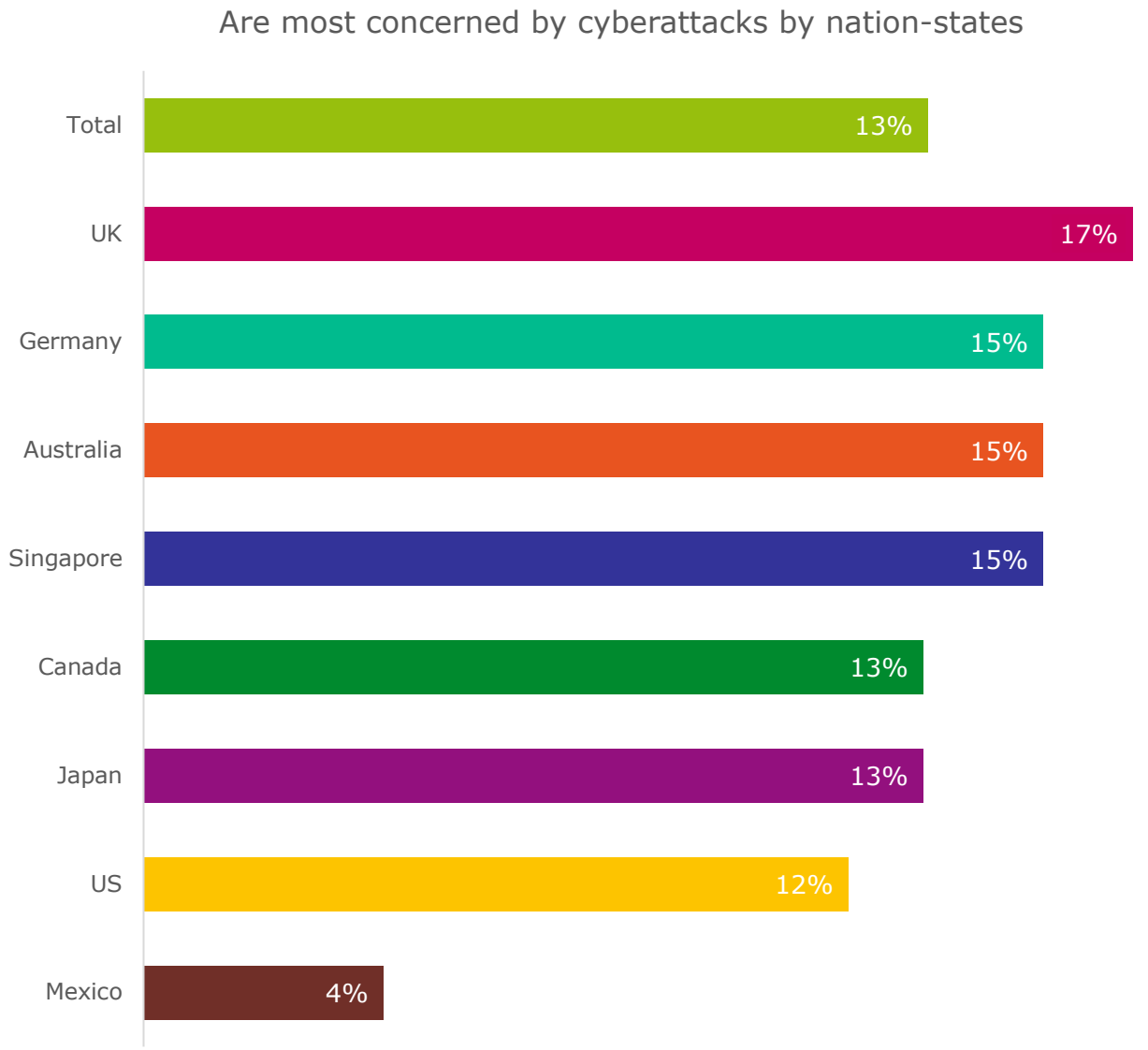
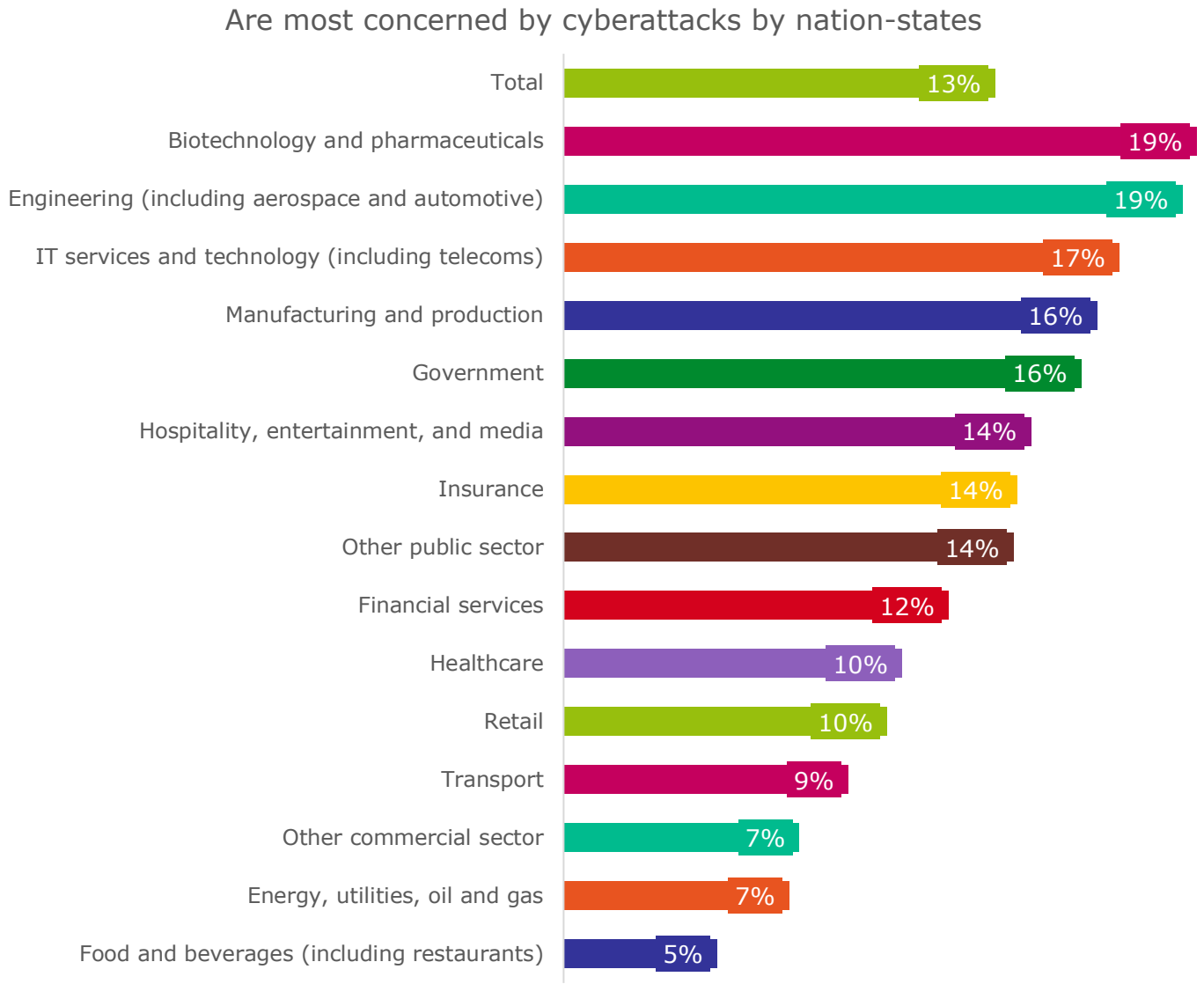


Figure 7: *Analysis showing the percentage of respondents who are most concerned by nation-states targeting their organization for cyberattack. Asked to all respondents, split by respondent country (1,300)*

VansonBourne

Attacks by nation-states



Some industries take the threat of nation-state attack more seriously than others

Figure 8: *Analysis showing the percentage of respondents who are most concerned by nation-states targeting their organization for cyberattack. Asked to all respondents, split by organization sector (1,300)*

VansonBourne

Security spending

89% agree

That investing in security can help their organization gain a competitive advantage

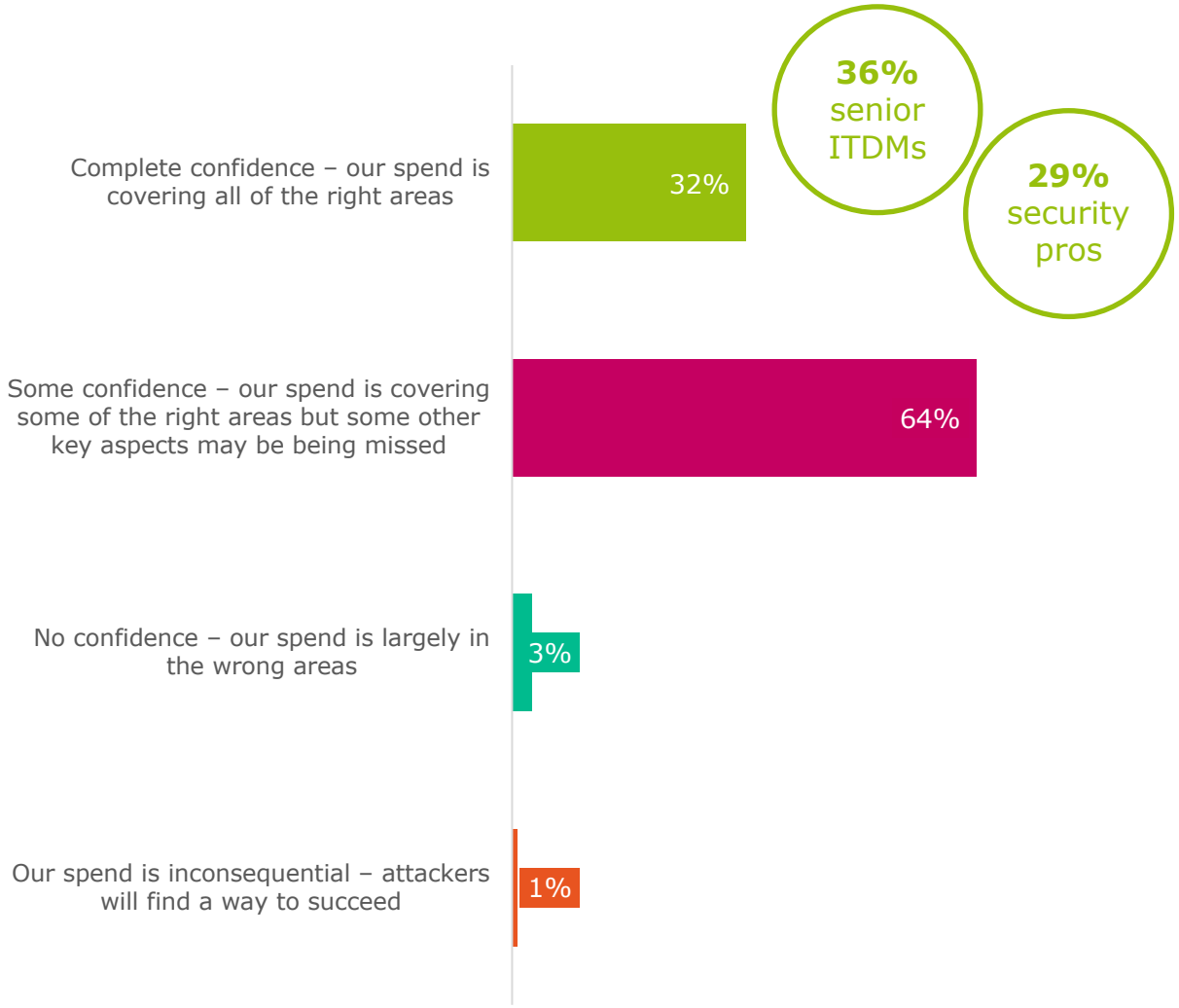


Figure 9: *Analysis showing the percentage of respondents that agree with the statement above. Asked to all respondents (1,300)*

Figure 10: "How confident are you that your organization is spending in the correct areas of IT security?" *asked to all respondents, showing the percentage of respondents that selected 'complete confidence' split by respondent type (1,300)*

VansonBourne

Putting security first

"Corporate security is more important than individual employee privacy"

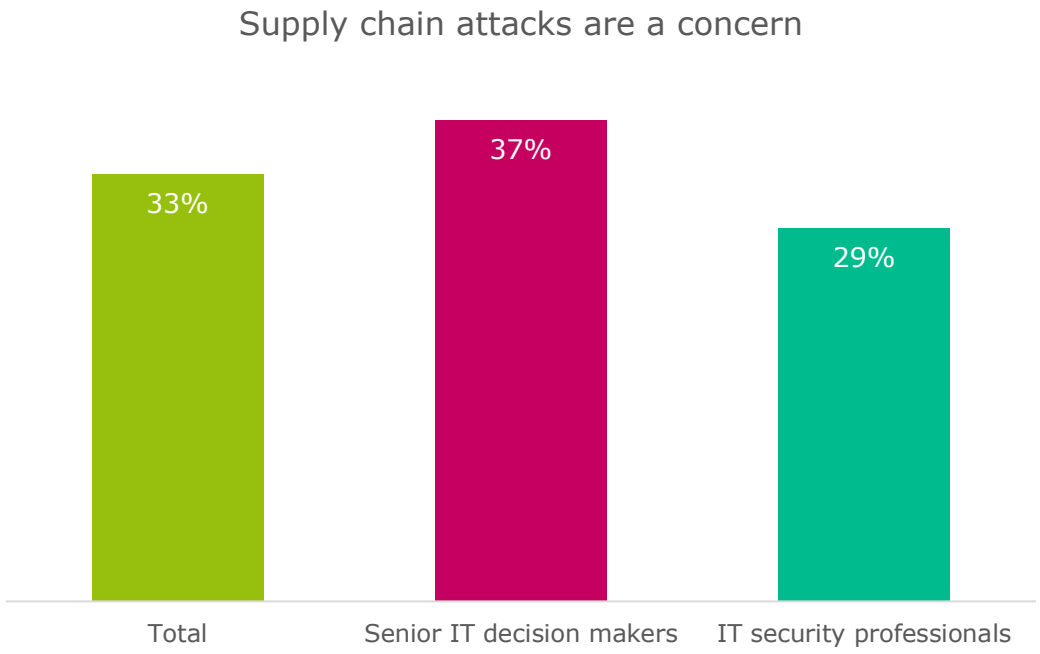
Figure 11: *Analysis showing the percentage of respondents that agree and disagree with the statement above. Asked to all respondents (1,300)*

VansonBourne

2: The security disruptor – supply chain attacks

VansonBourne

Supply chain attacks in respondents' minds



"We still have work to do before we are prepared to defend against supply chain attacks"

Figure 12: *Analysis showing the percentage of respondents who see supply chain attacks (such as NotPetya) as a concern for their organization over the next 12 months. Asked to all respondents, split by respondent type (1,300)*

Figure 13: *Analysis showing the percentage of respondents who think that their organization still has either a long way to go, or some way to go, before they are fully prepared to defend against supply chain attacks. Asked to all respondents, split by respondent type (1,300)*

VansonBourne

Top areas of IT security focus

Protecting data and IP (59%) or early attack detection (59%) are among the top security focuses for nearly six in ten

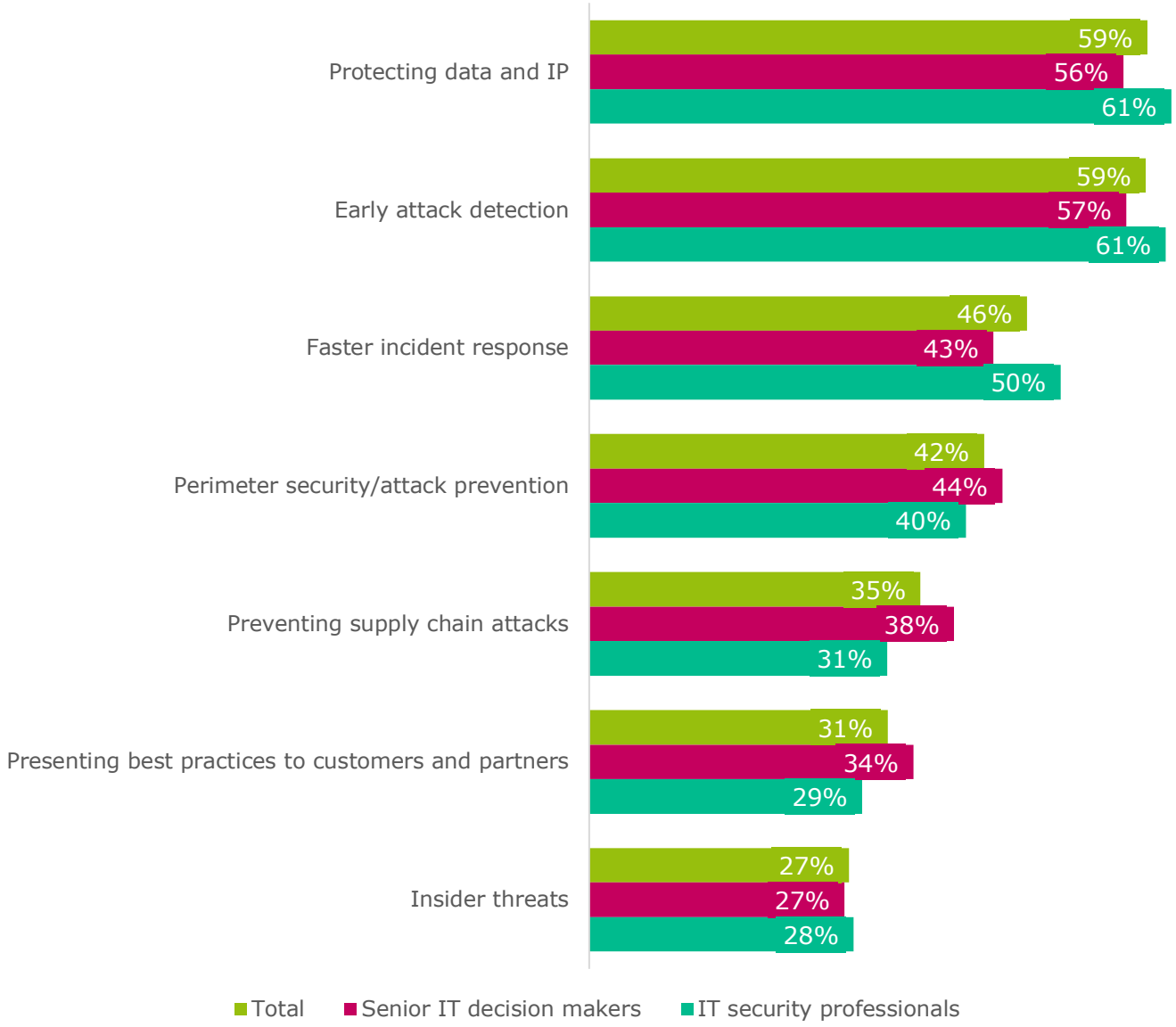


Figure 14: "In your opinion, what is your organization's focus when it comes to IT security?" *asked to all respondents, showing a combination of the first, second, and third biggest IT security focuses, split by respondent type (1,300)*

VansonBourne

Spending on software supply chain security

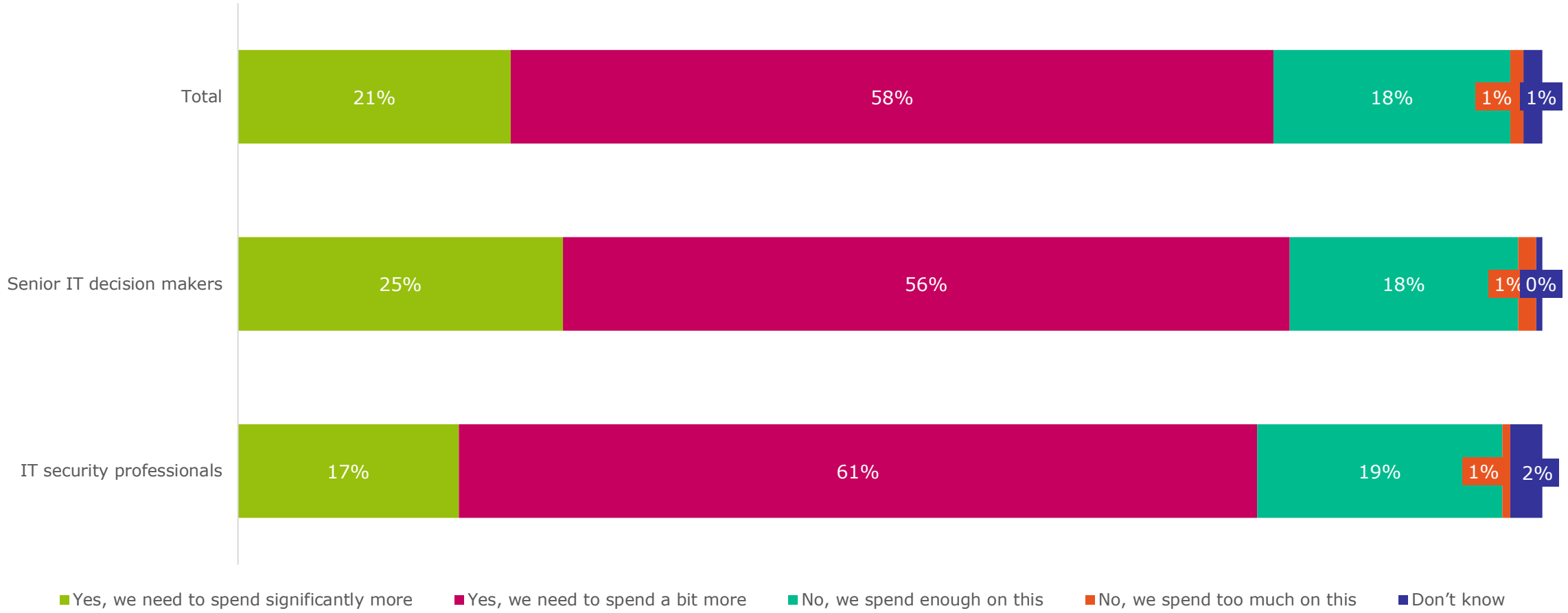


Figure 15: "In your opinion, should your organization be spending more on software supply chain security?" *asked to all respondents , split by respondent type (1,300)*

VansonBourne

Thinking about supply chain security

Figure 16: *Analysis showing the percentage of respondents that agree with the statements listed above. Asked to all respondents (1,300)*

VansonBourne

3: Eliminating the weakest link

VansonBourne

Responding to a software supply chain attack

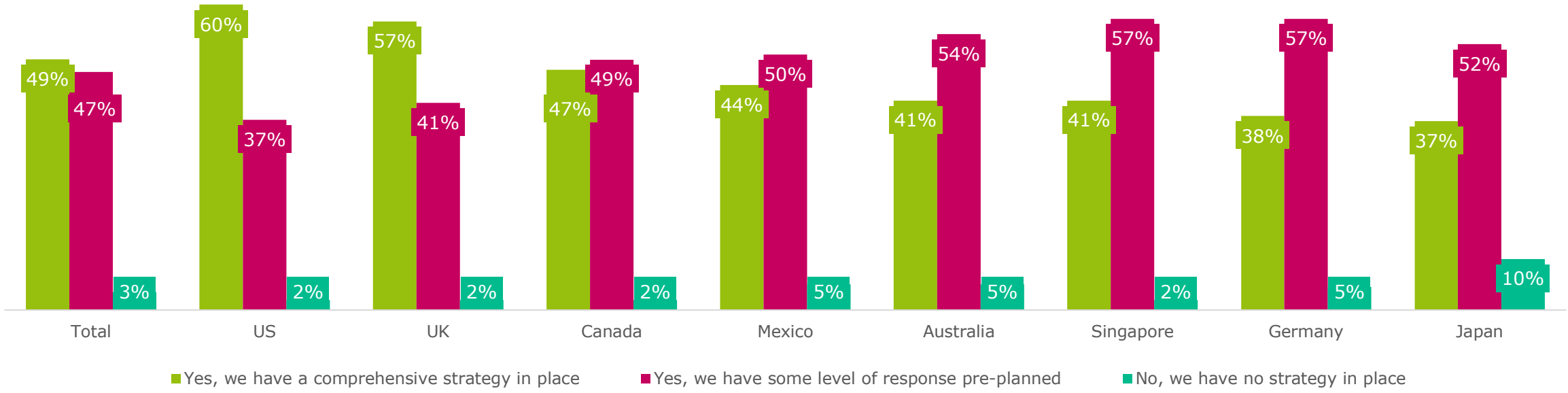


Figure 19: "Does your organization have a plan or strategy in place to coordinate your response should it be breached by software supply chain attack?" *asked to all respondents, but not showing 'don't know' responses, split by respondent country (1,300)*

VansonBourne

Using new technology to fight supply chain attacks

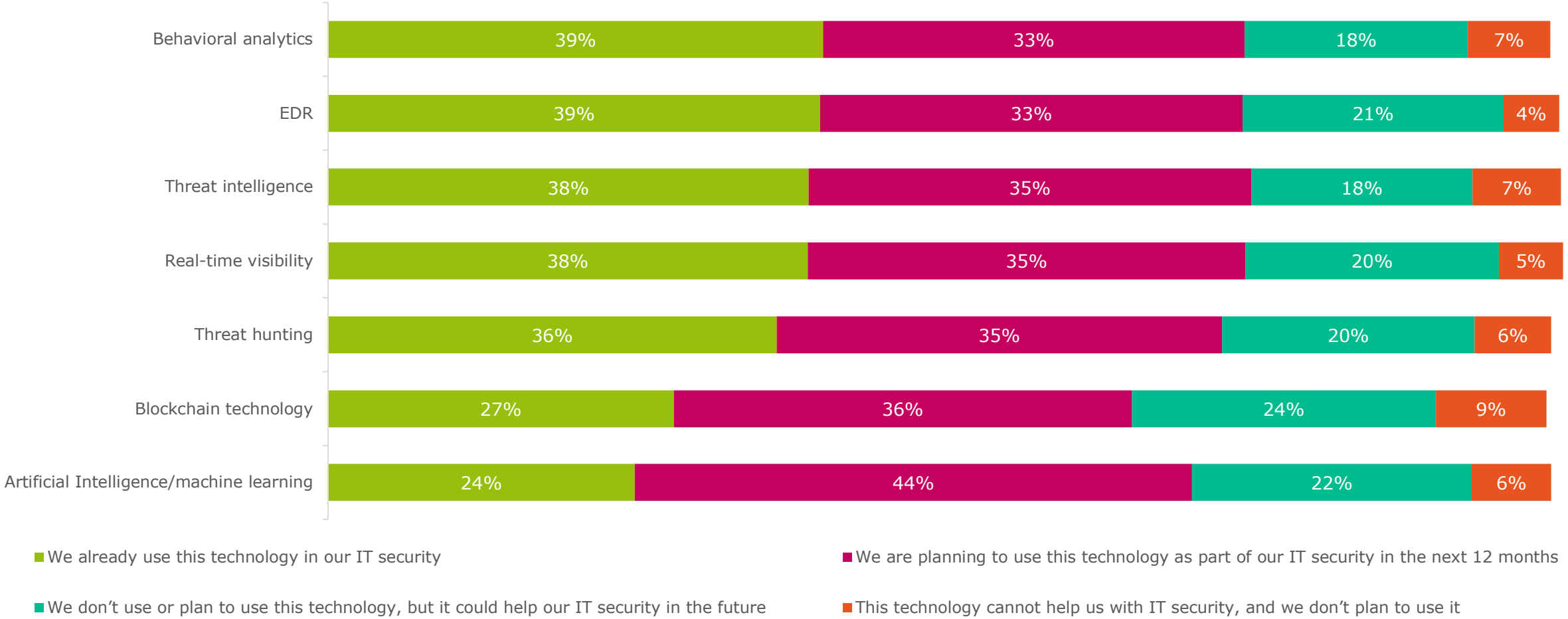


Figure 20: "Do you think that any of the following emerging technologies will be of particular benefit when trying to protect your organization against software supply chain attacks, and does your organization employ any already?" *asked to all respondents, but not showing 'don't know' responses (1,300)*

VansonBourne

Attitude to suppliers

80%
agree

*"My organization would **avoid working with** emerging, or less established vendors due to a perceived weakness in security strategy"*

*"My organization does not always **hold external suppliers to the same security standards** as we hold ourselves"*

72%
agree

Figure 21: *Analysis showing the percentage of respondents who agree with the statements shown above. Asked to all respondents (1,300)*

VansonBourne

Vetting suppliers

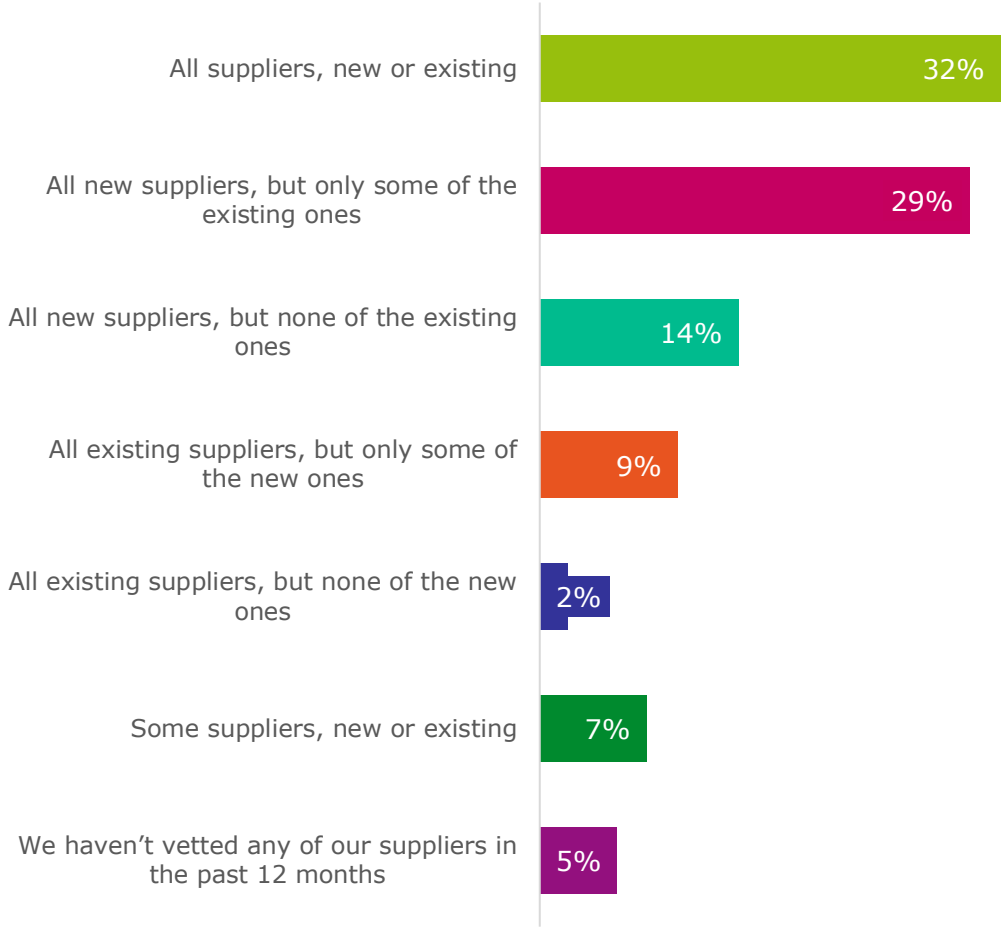


Figure 22: "How many of your organization's software suppliers have been vetted for security purposes in the past 12 months?" *asked to all respondents (1,300)*

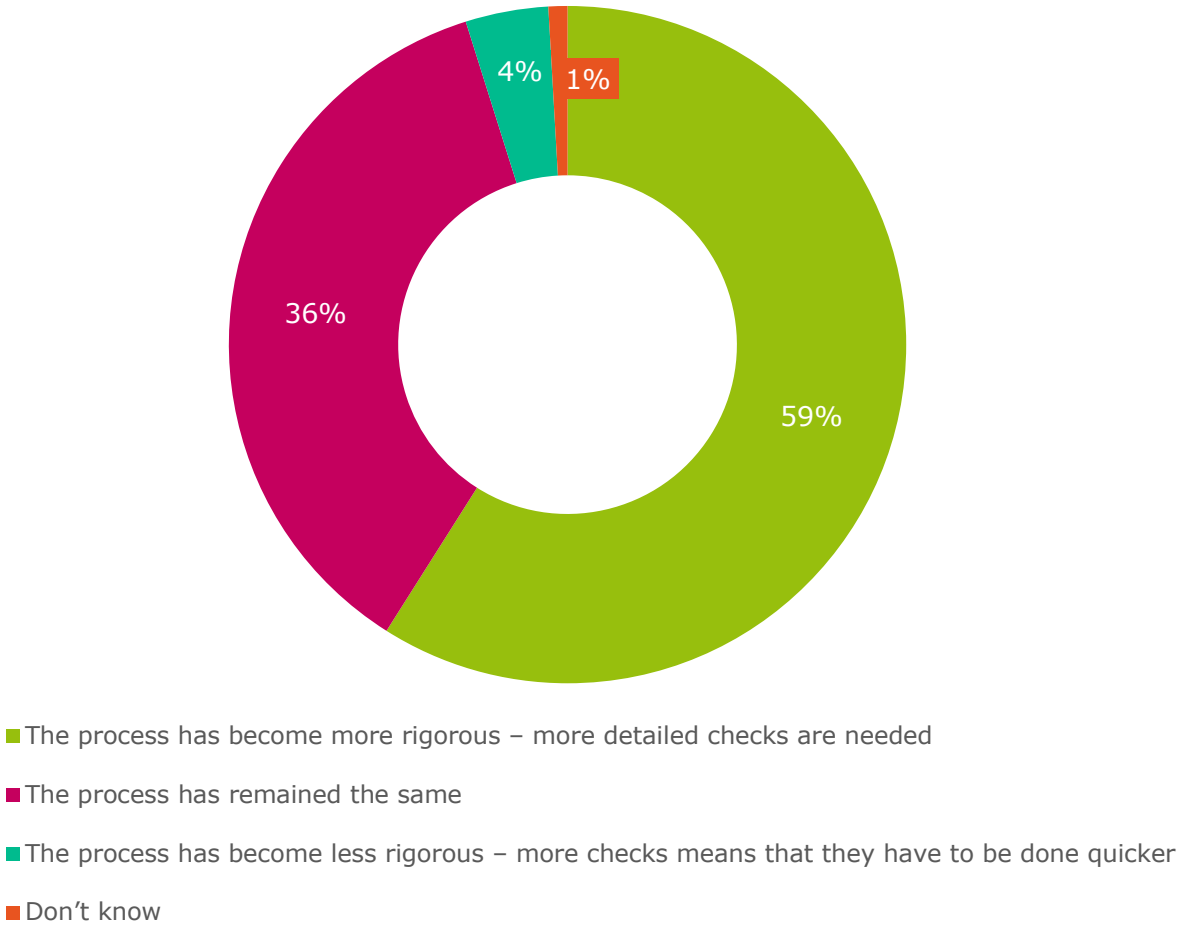


Figure 23: "Has your organization's vetting process changed in the wake of recent high profile supply chain attacks such as NotPetya and WannaCry?" *asked to respondents whose organization has vetted suppliers in the past 12 months (1,214)*

VansonBourne

The level of vetting in different countries

In no country has the majority of respondents' organizations vetted all suppliers, new or existing, over the past 12 months

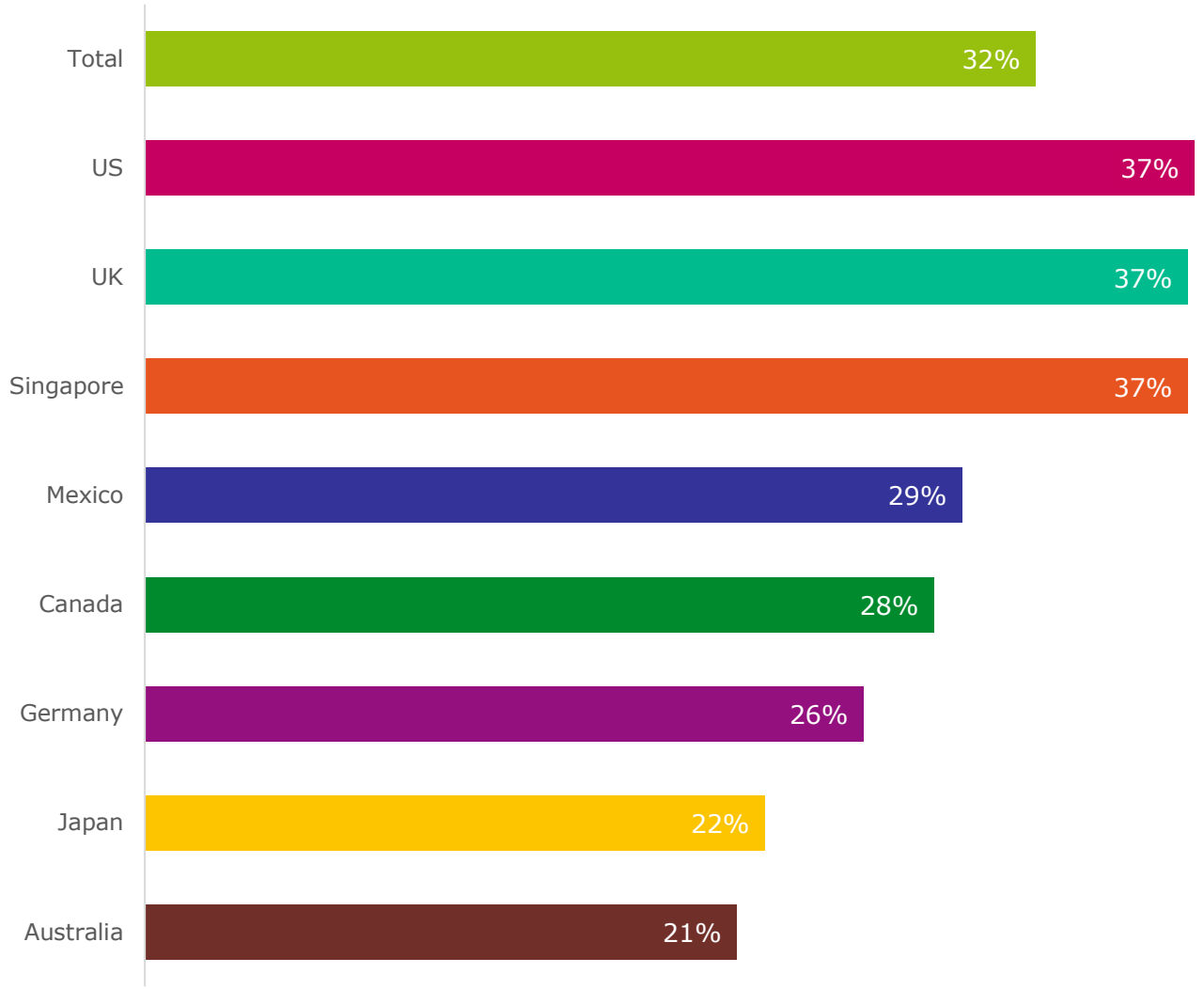


Figure 24: *Analysis showing the percentage of respondents whose organization has vetted all suppliers, new or existing, in the past 12 months. Asked to all respondents, split by respondent country (1,300)*

VansonBourne

Security and new suppliers

87%
agree

"Security is a critical factor when making purchasing decisions surrounding new suppliers"

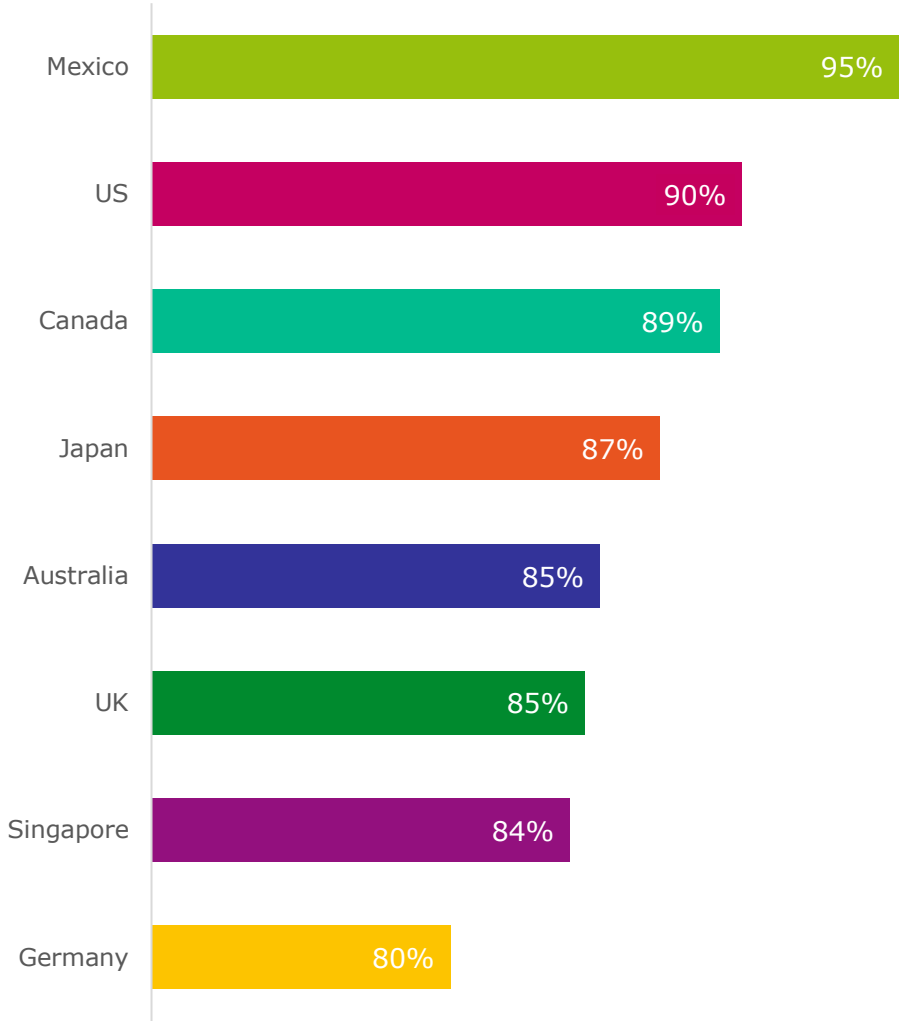
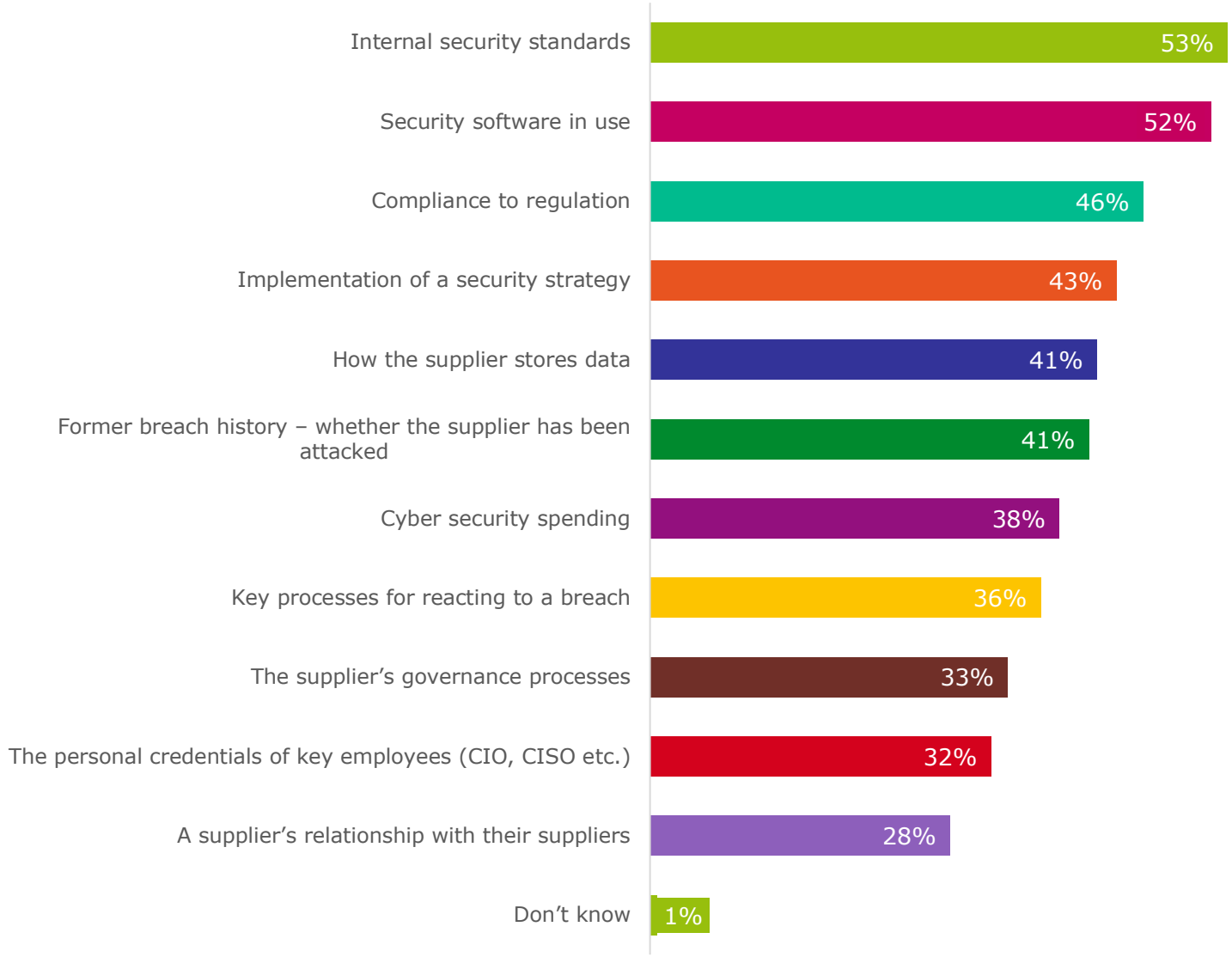


Figure 25: *Analysis showing the percentage of respondents who agree with the statement above. Asked to all respondents, split by respondent country (1,300)*

VansonBourne

What to look for when vetting a supplier



Just over half of respondents' organizations look at a suppliers internal security standards (53%) or their security software in use (52%) when vetting a supplier, new or existing

Figure 26: "When vetting a supplier, new or existing, what does your organization check for?" *asked to respondents whose organization has vetted suppliers in the past 12 months (1,214)*

VansonBourne

Board involvement in supply chain security

Only 5% have not seen a change in attitude toward software supply chain attacks from their board since the high profile NotPetya and WannaCry attacks

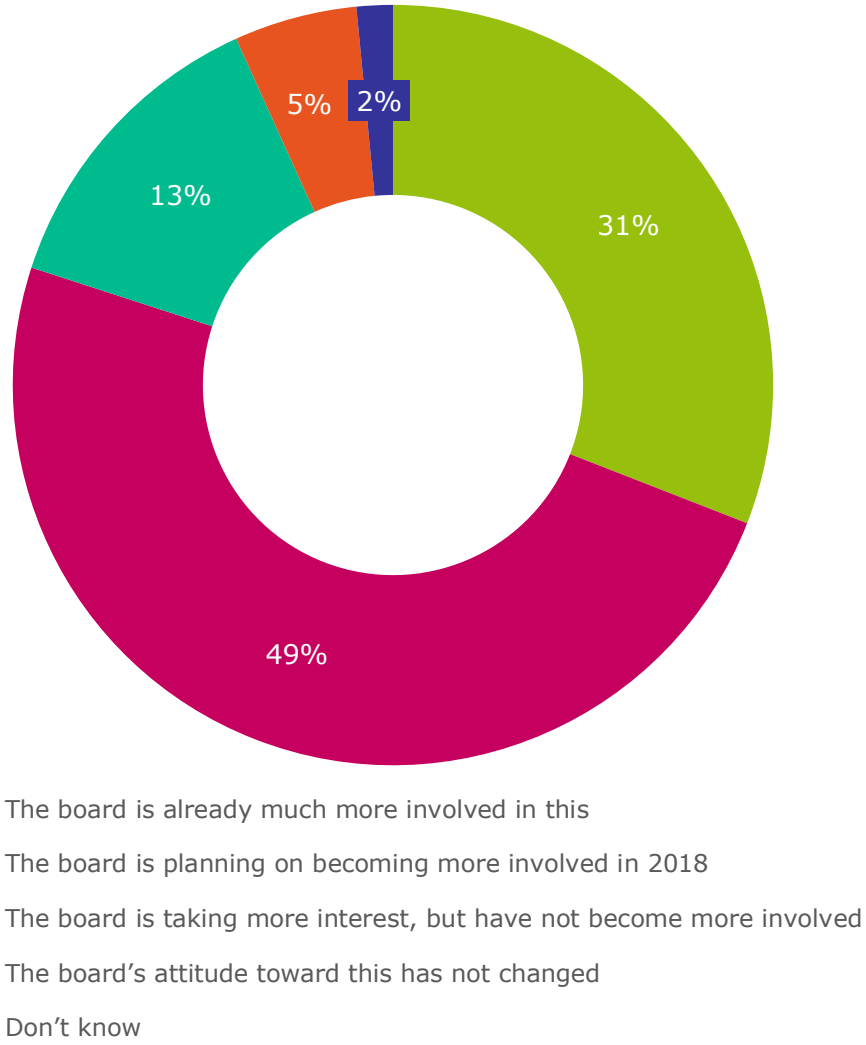


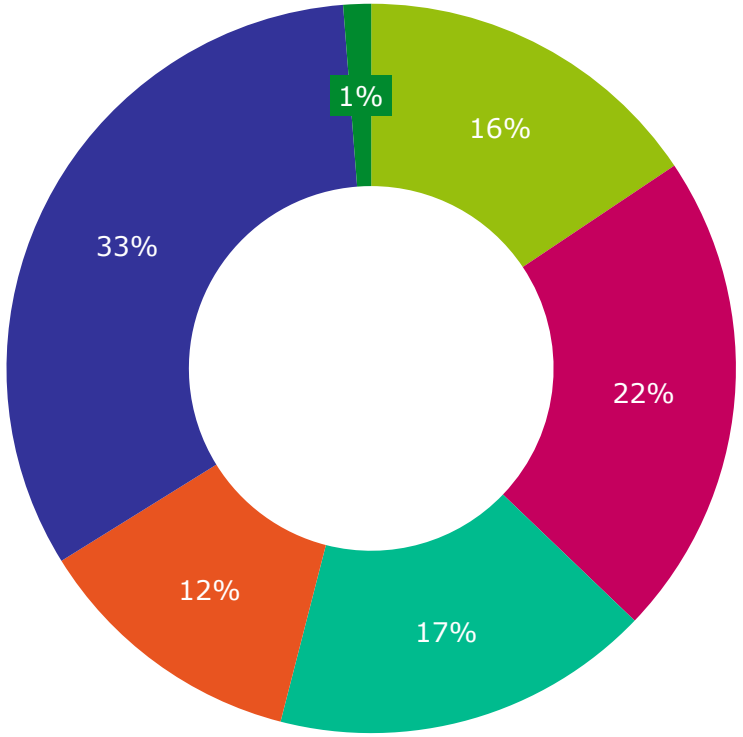
Figure 27: "Has the level of involvement/interest in software supply chain security from your organization's board changed in the wake of the high profile NotPetya and WannaCry attacks in 2017?" *asked to all respondents (1,300)*

VansonBourne

4: When the chain breaks

VansonBourne

Experiencing a software supply chain attack



Two thirds (66%) or organizations have experienced a software supply chain attack at some point – 32% within the last 12 months

Figure 28: "Has your organization ever experienced a software supply chain attack?" *asked to all respondents (1,300)*

- Yes, on several occasions, including within the last 12 months
- Yes, on several occasions, but not in the last 12 months
- Yes, once, within the last 12 months
- Yes, once, but not in the last 12 months
- No, we have never experienced this type of attack
- Don't know

VansonBourne

Experiencing a software supply chain attack

Experienced a software supply chain attack

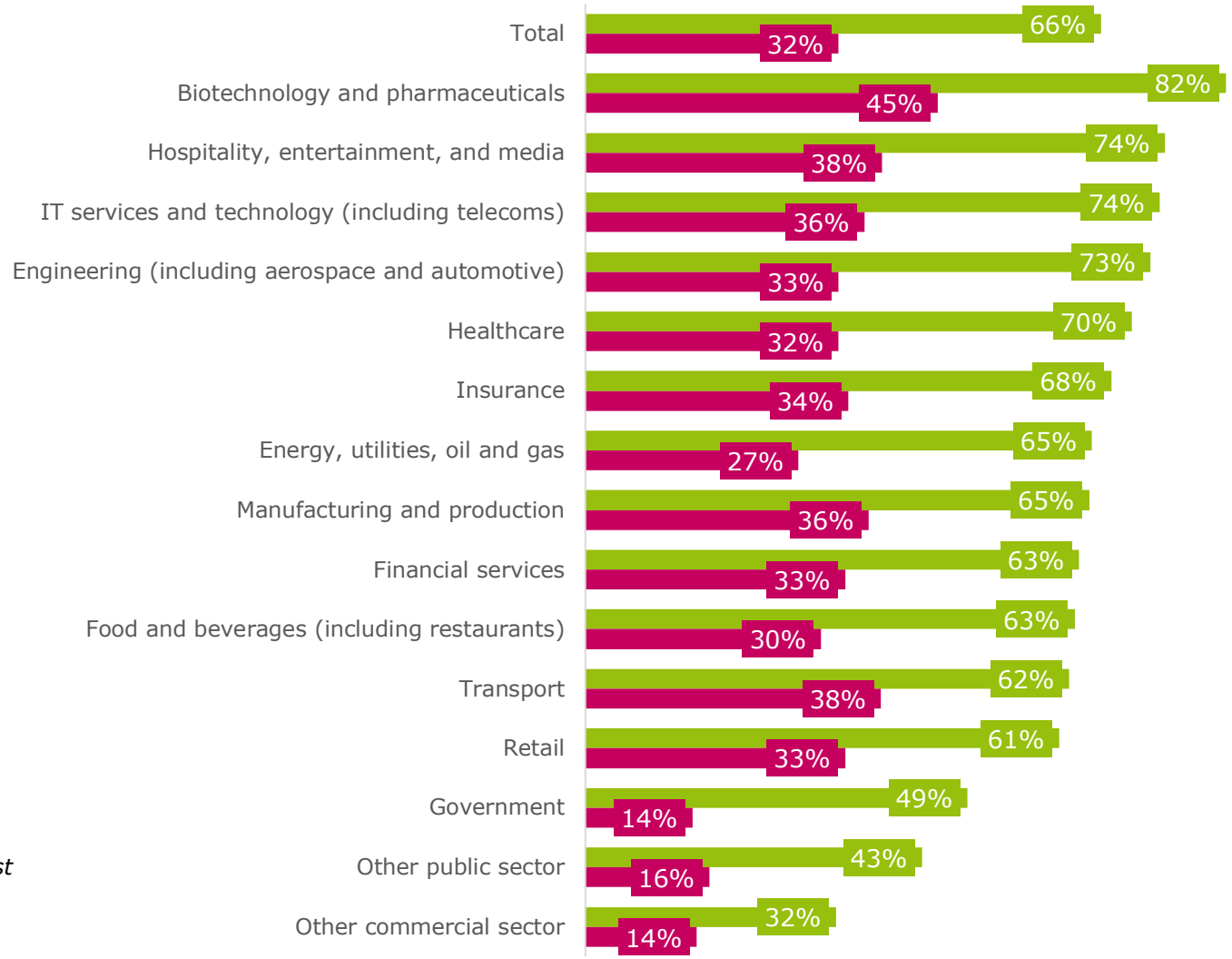


Figure 29: *Analysis showing the percentage of respondents whose organization has experienced a software supply chain attack at any point, or within the last 12 months. Asked to all respondents, split by organization sector (1,300)*

VansonBourne

Response time

Average number of hours respondents' organizations would take to…

Detect	React	Respond	Remediate
10:00	13:00	15:00	25:00

…a software supply chain attack

Figure 30: *Analysis showing the average number of hours respondents' organizations would take to detect/react/respond/remediate a software supply chain attack. Asked to all respondents (1,300)*

Time to take action, by country

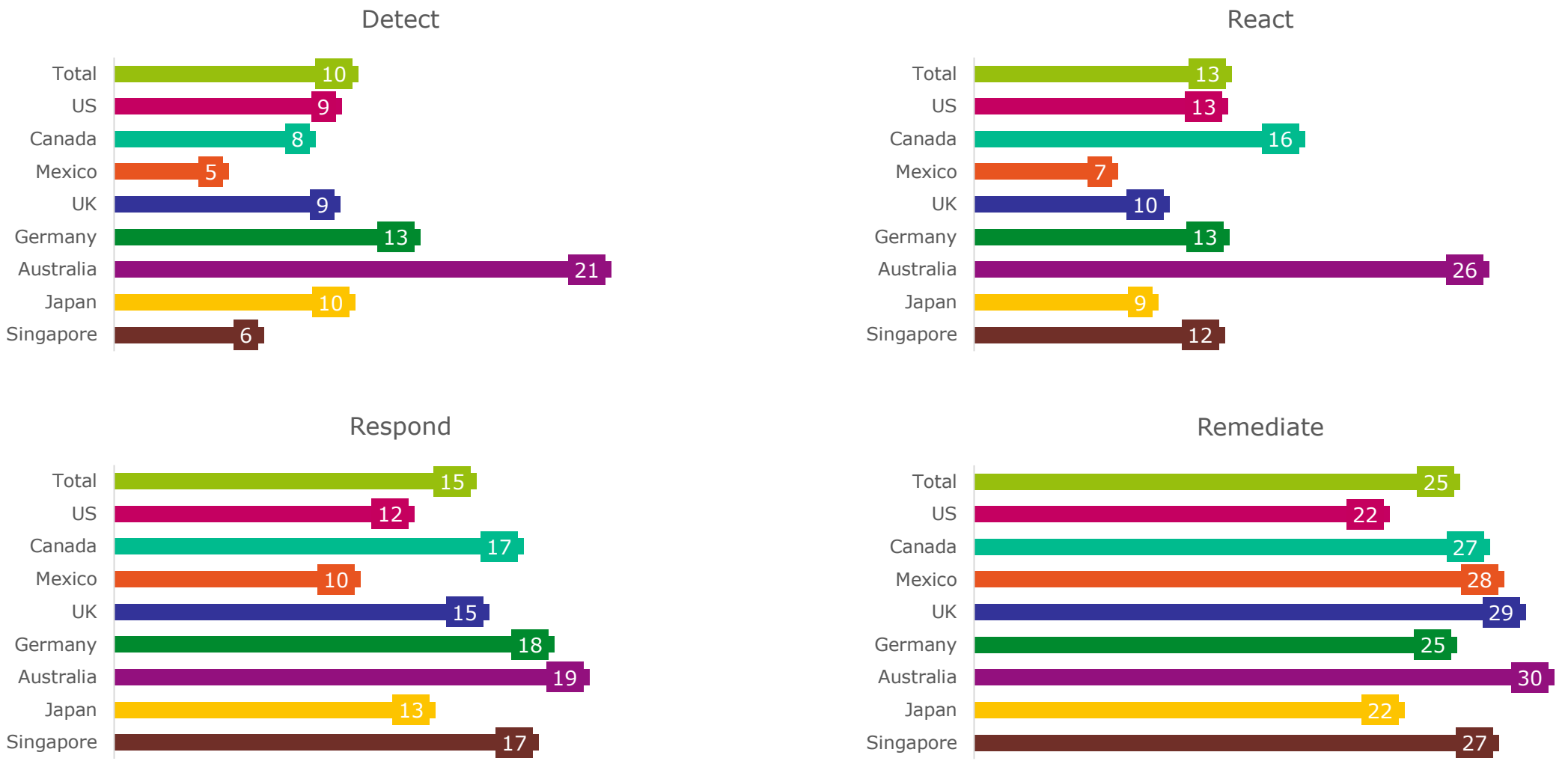


Figure 31: *Analysis showing the average time taken (in hours) to detect, react, respond, and remediate a software supply chain attack. Asked to all respondents, split by respondent country (1,300)*

VansonBourne

Time to take action, by sector

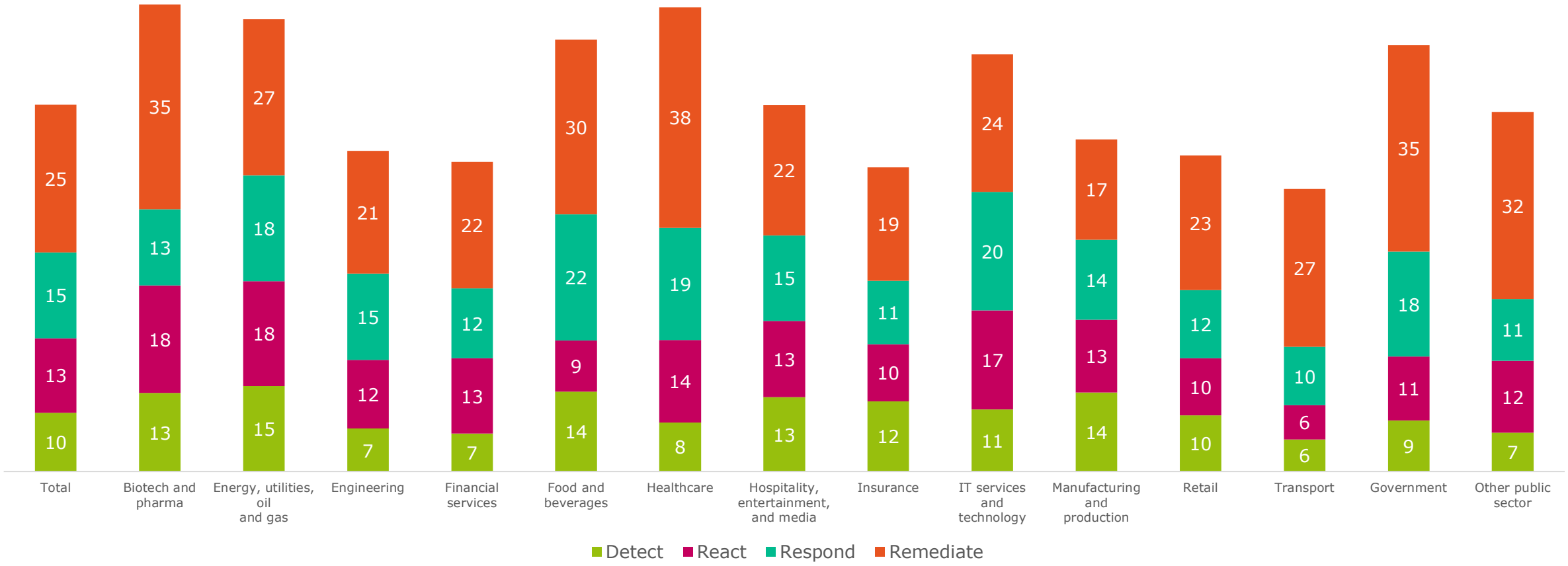


Figure 32: *Analysis showing the average time taken (in hours) to detect, react, respond, and remediate a software supply chain attack. Asked to all respondents, split by organization sector (1,300)*

VansonBourne

Financial cost of a software supply chain attack

incurred a financial cost as a result of experiencing their a software supply chain attack

Average cost of the last software supply chain attack experienced by respondents' organizations (USD $)

$1,124,914

Figure 33: *Analysis showing the percentage of respondents' organizations that incurred a financial cost as a result of experiencing their last software supply chain attack. Asked to respondents whose organization has experienced a software supply chain attack (860)*

Figure 34: *Analysis showing the average cost of the last software supply chain attack experienced by respondents' organizations (USD $). Asked to respondents whose organization has experienced a software supply chain attack (860)*

VansonBourne

Losing more than just money

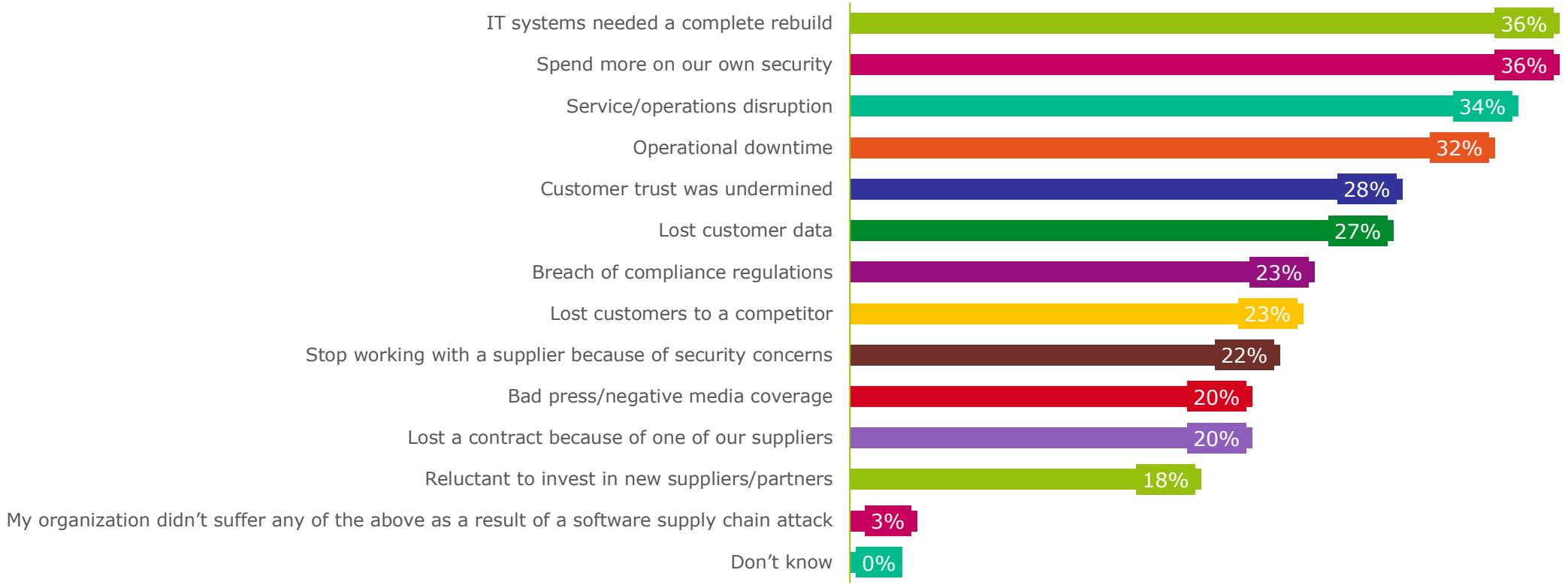


Figure 37: "Excluding financial loss, has your organization experienced any of the following drawbacks as a result of suffering a software supply chain attack?" *asked to respondents whose organization has experienced a software supply chain attack (860)*

Nearly all (97%) of those organizations that suffered a supply chain attack, experienced drawbacks, excluding financial loss

VansonBourne

Response strategy in place?

The vast majority (87%) of those that suffered a supply chain attack had either a full strategy in place, or some level of response pre-planned at the time of their attack

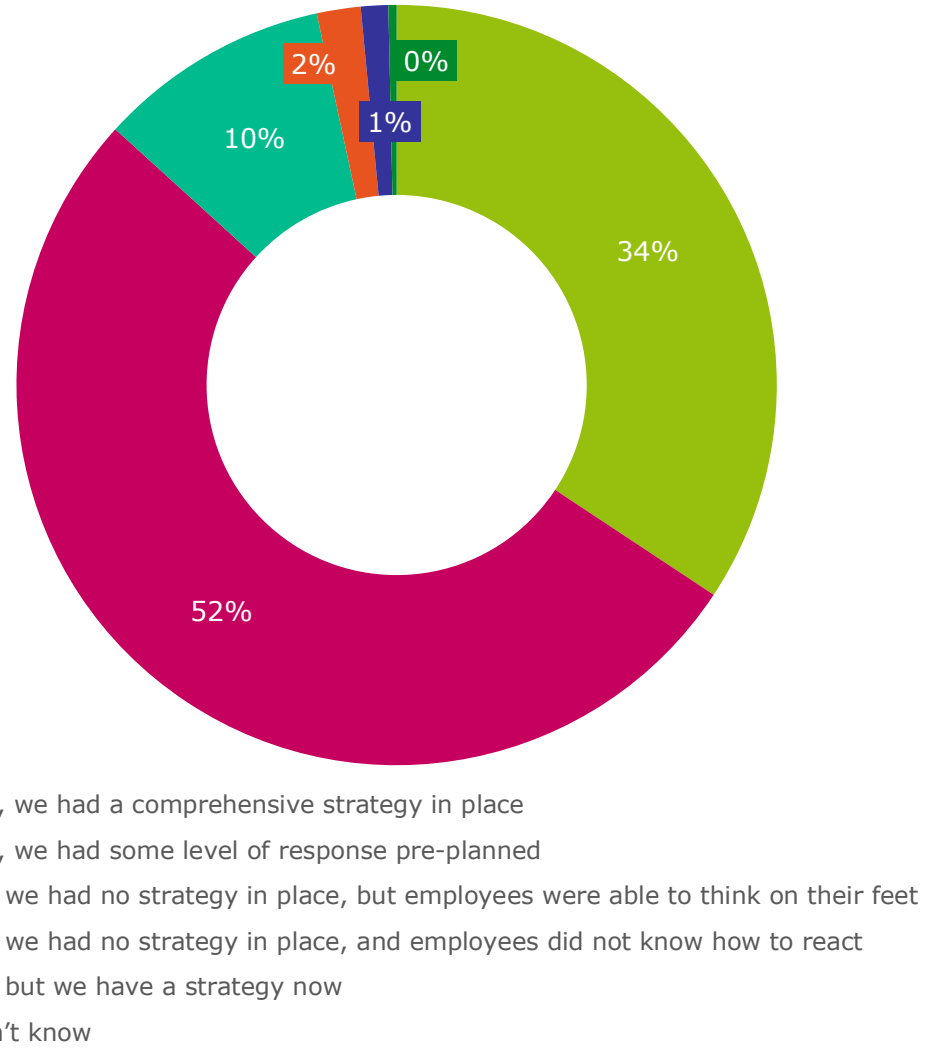


Figure 38: "When your organization suffered its first software supply chain attack/s, did you have a plan or strategy in place to coordinate your response?" *asked to respondents whose organization has experienced a software supply chain attack (860)*

VansonBourne

Paying a ransom to recover data

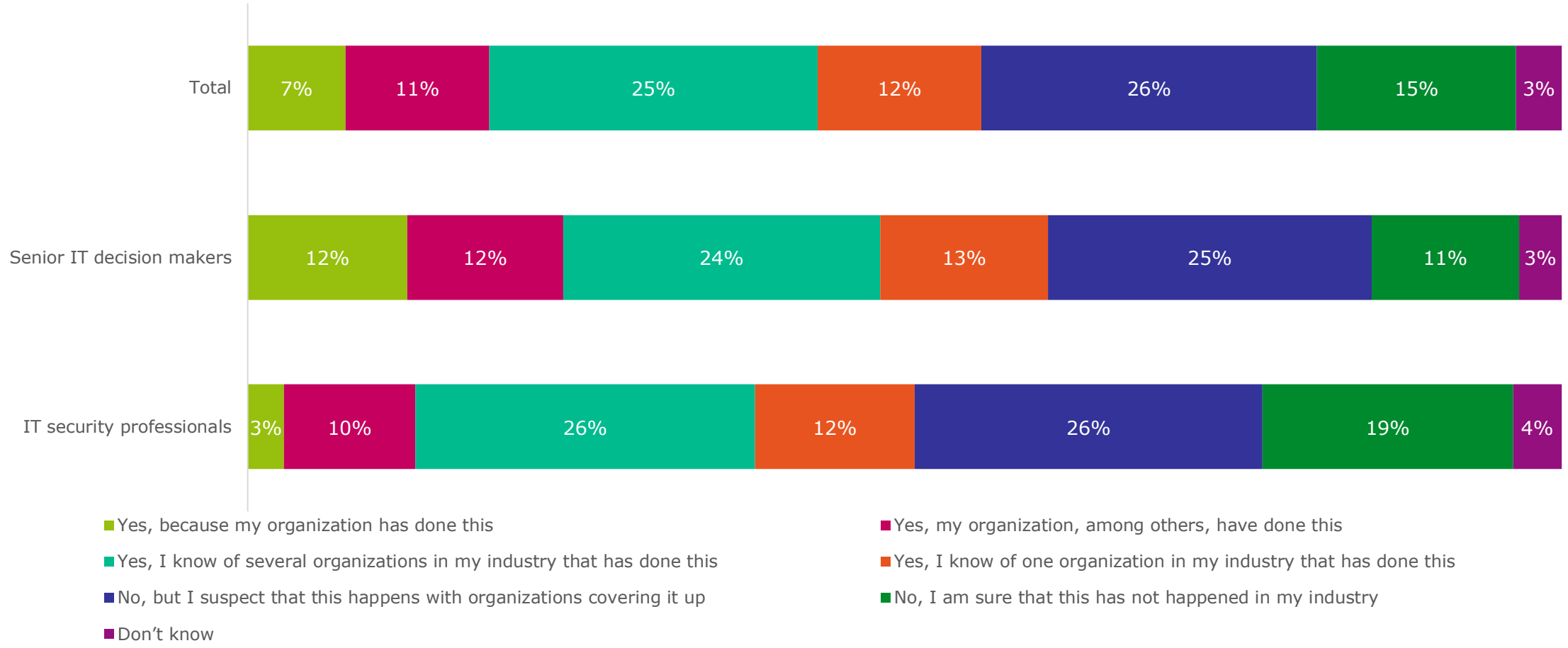


Figure 39: "Do you know of any organizations within your industry that has paid a ransom to cyber attackers in order to recover data encrypted in a software supply chain attack in the past 12 months?" *asked to all respondents, split by respondent type (1,300)*

VansonBourne

Confidence in the supply chain

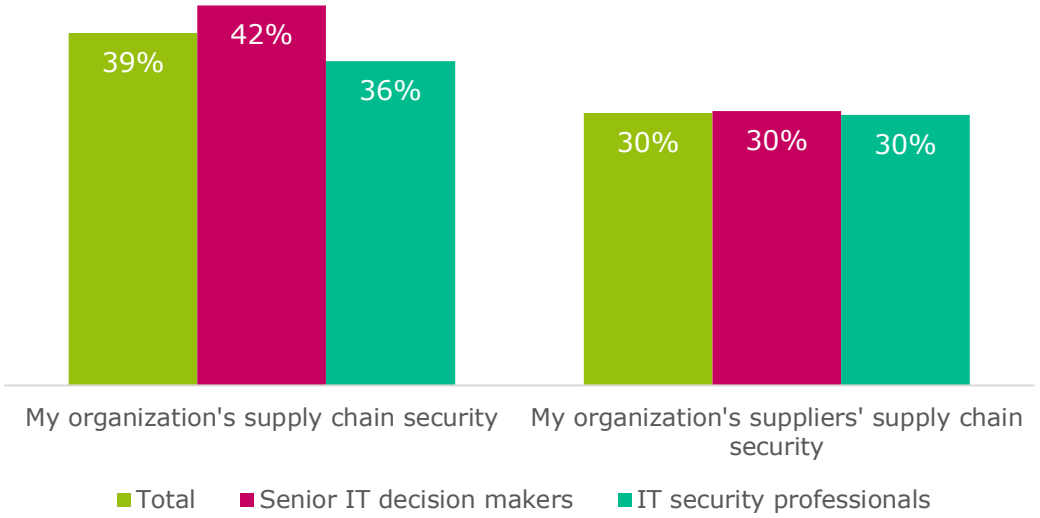


Figure 40: *Analysis showing the percentage of respondents who personally have total confidence in the IT security of their organization's supply chain. Asked to all respondents, split by respondent type (1,300)*

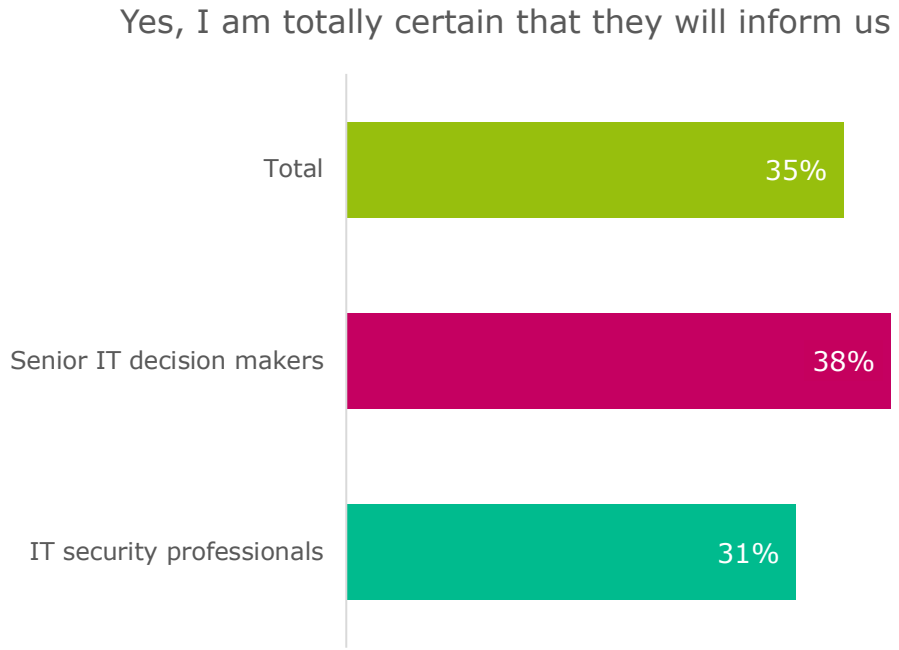


Figure 41: *Analysis showing the percentage of respondents who are totally certain that their organization's suppliers or partners will inform them if they are ever breached by a successful cyberattack. Asked to all respondents, split by respondent type (1,300)*

Only three in ten (30%) respondents have total confidence in the IT security of their suppliers' suppliers

And a similarly low (35%) proportion are totally certain that suppliers will inform them if they are breached

VansonBourne

Trust in suppliers and security partners

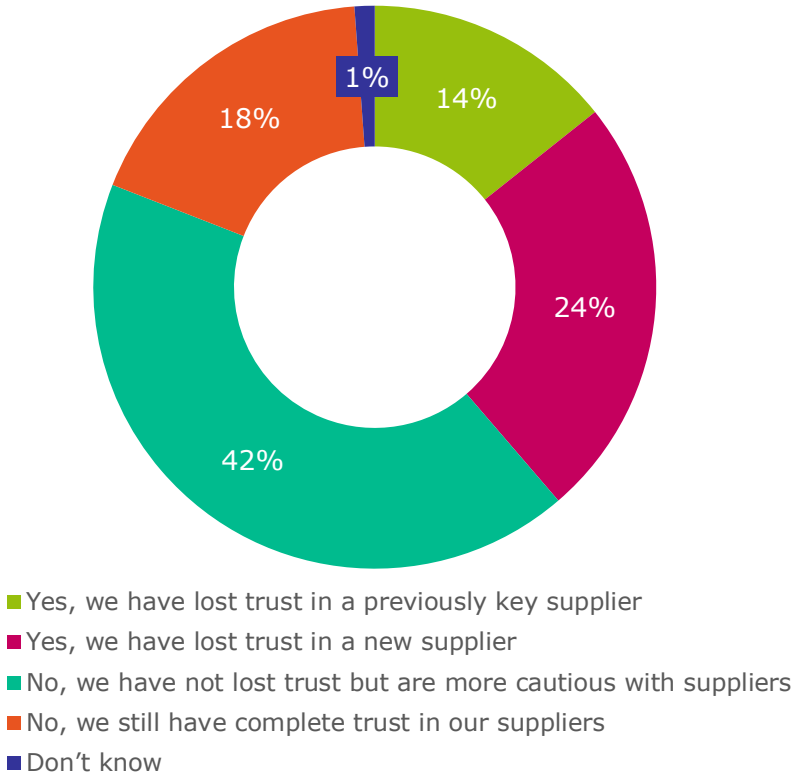


Figure 42: "Has your organization had any reason to lose trust in any of its key suppliers in the past 12 months?" *asked to all respondents (1,300)*

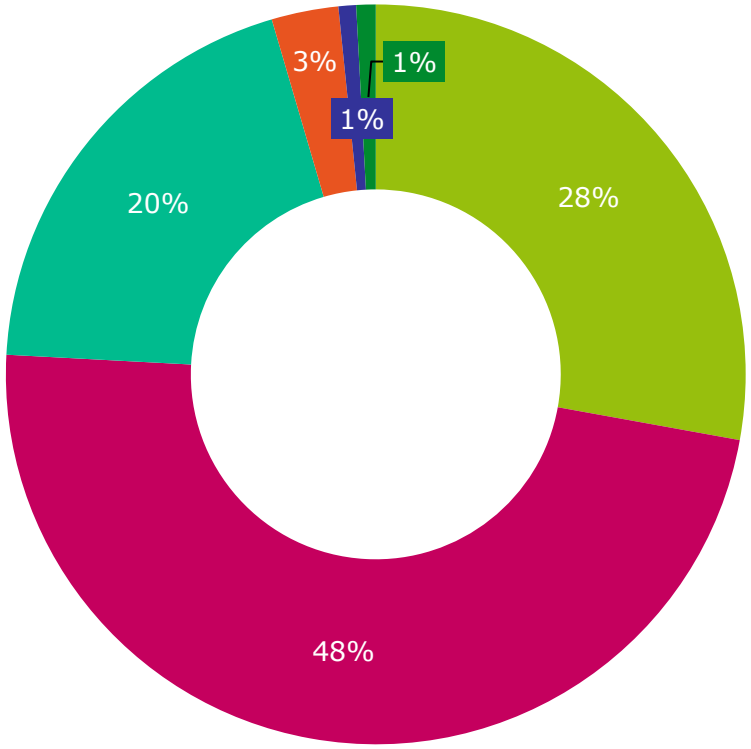
Some have lost trust in new, or even key, suppliers in the past 12 months

GDPR will impact the evaluation of security partners

Figure 43: "In your opinion, is the EU's General Data Protection Regulation (GDPR) impacting your evaluation of potential security partners?" *asked to all respondents, split by respondent type (1,300)*

VansonBourne

Desire to increase supply chain resilience



Over a quarter (28%) of respondents see it as a certainty that they will become more resilient to supply chain attacks

Figure 44: "To what extent will your organization become more resilient to supply chain attacks over the next 12 months?" *asked to all respondents (1,300)*

VansonBourne

Securing the supply chain

CrowdStrike
Research results

June 2018

VansonBourne

Country splits

The level of agreement with the previous three statements varies by country…

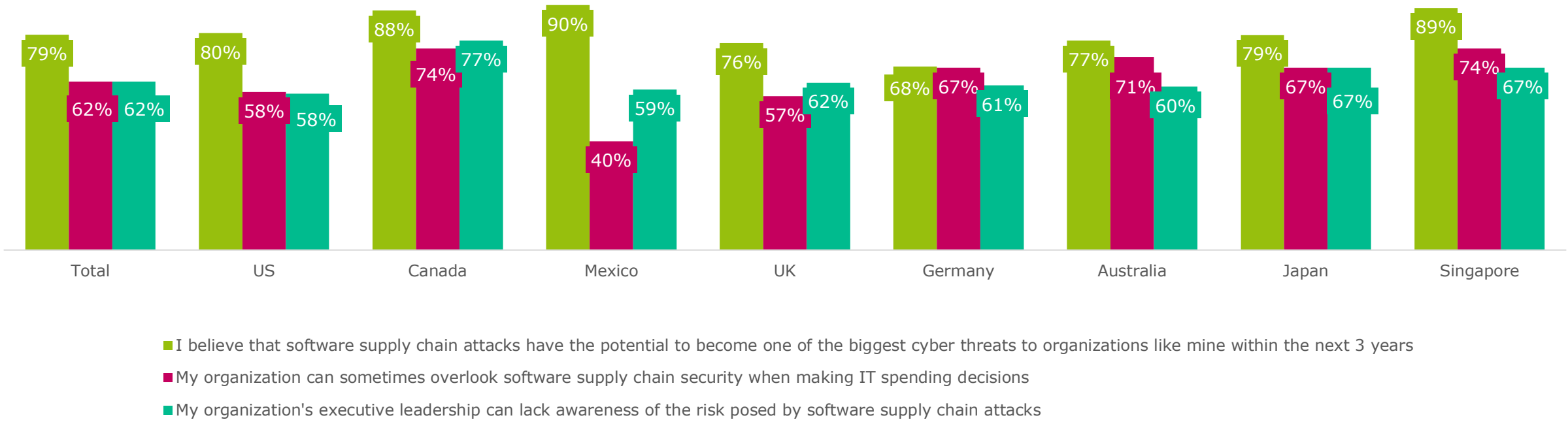


Figure 17: *Analysis showing the percentage of respondents who agree with the statements above. Asked to all respondents, split by respondent country (1,300)*

VansonBourne

Sector splits

…and by sector

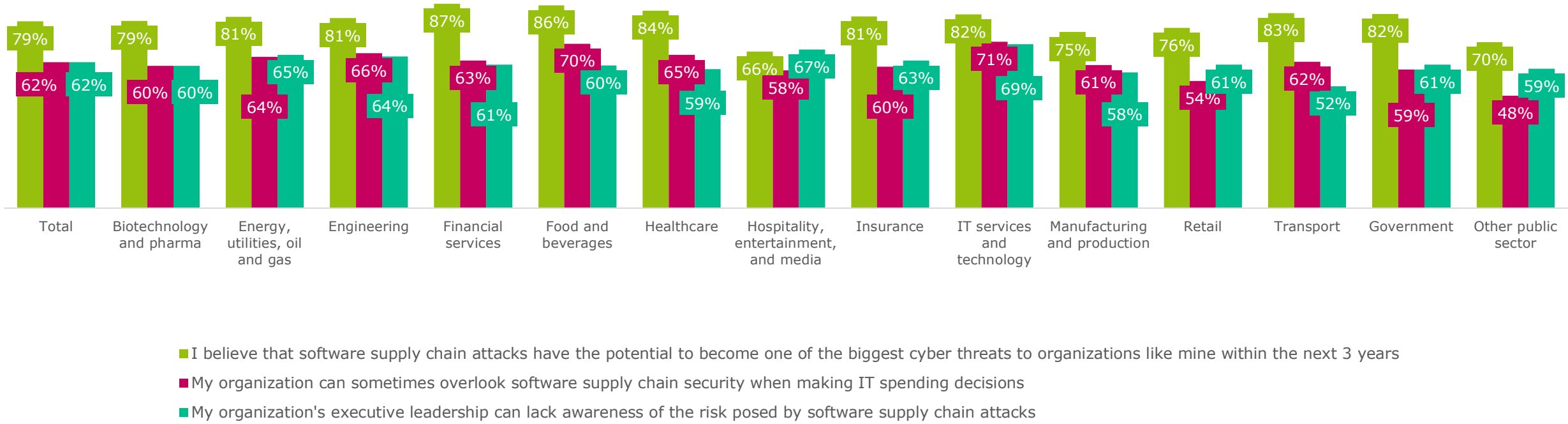


Figure 18: *Analysis showing the percentage of respondents who agree with the statements above. Asked to all respondents, split by organization sector, and excluding 'other commercial sector' (1,300)*

VansonBourne

Cost of a software supply chain attack

The cost of suffering a supply chain attack can vary depending on the sector of the organization

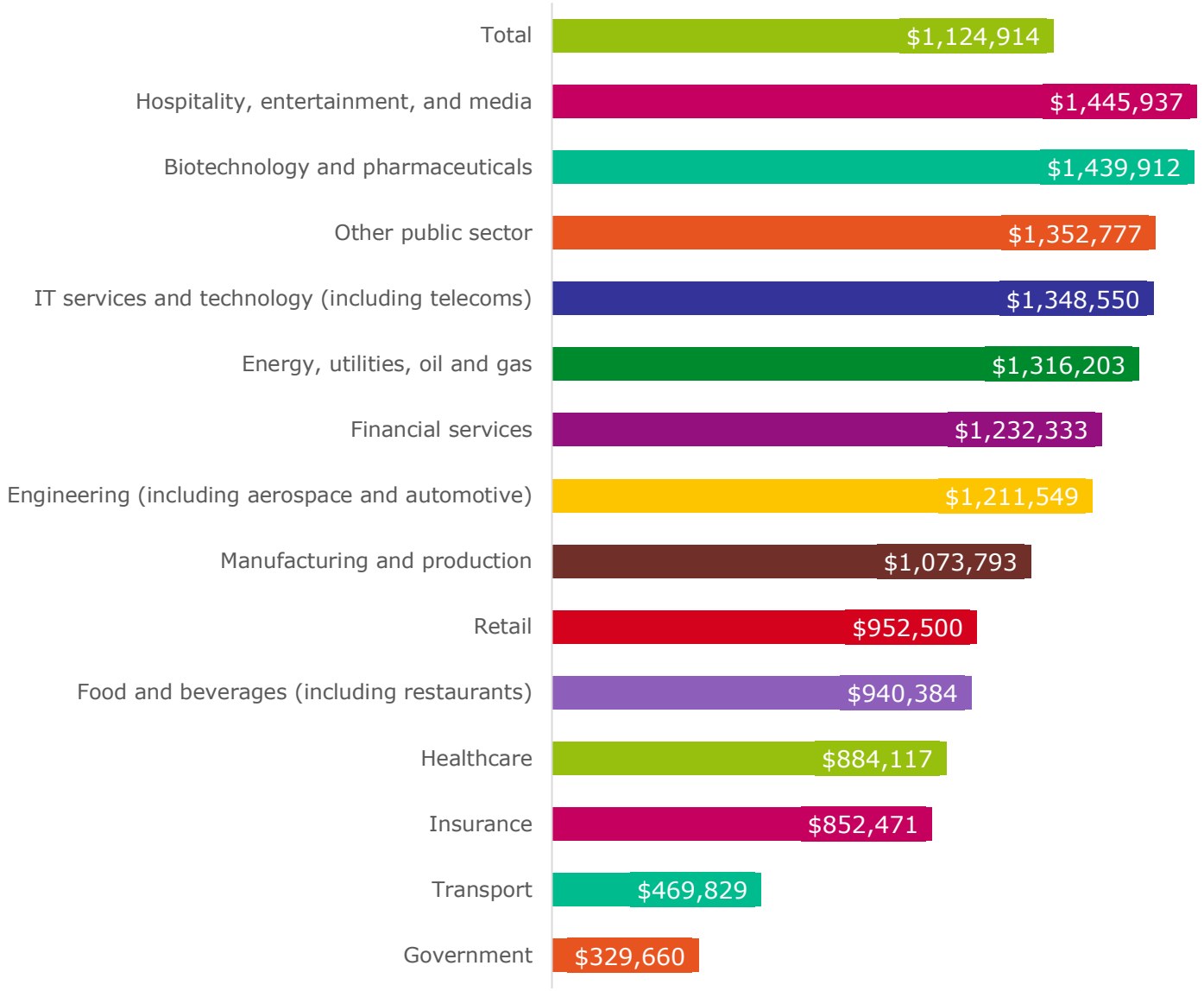
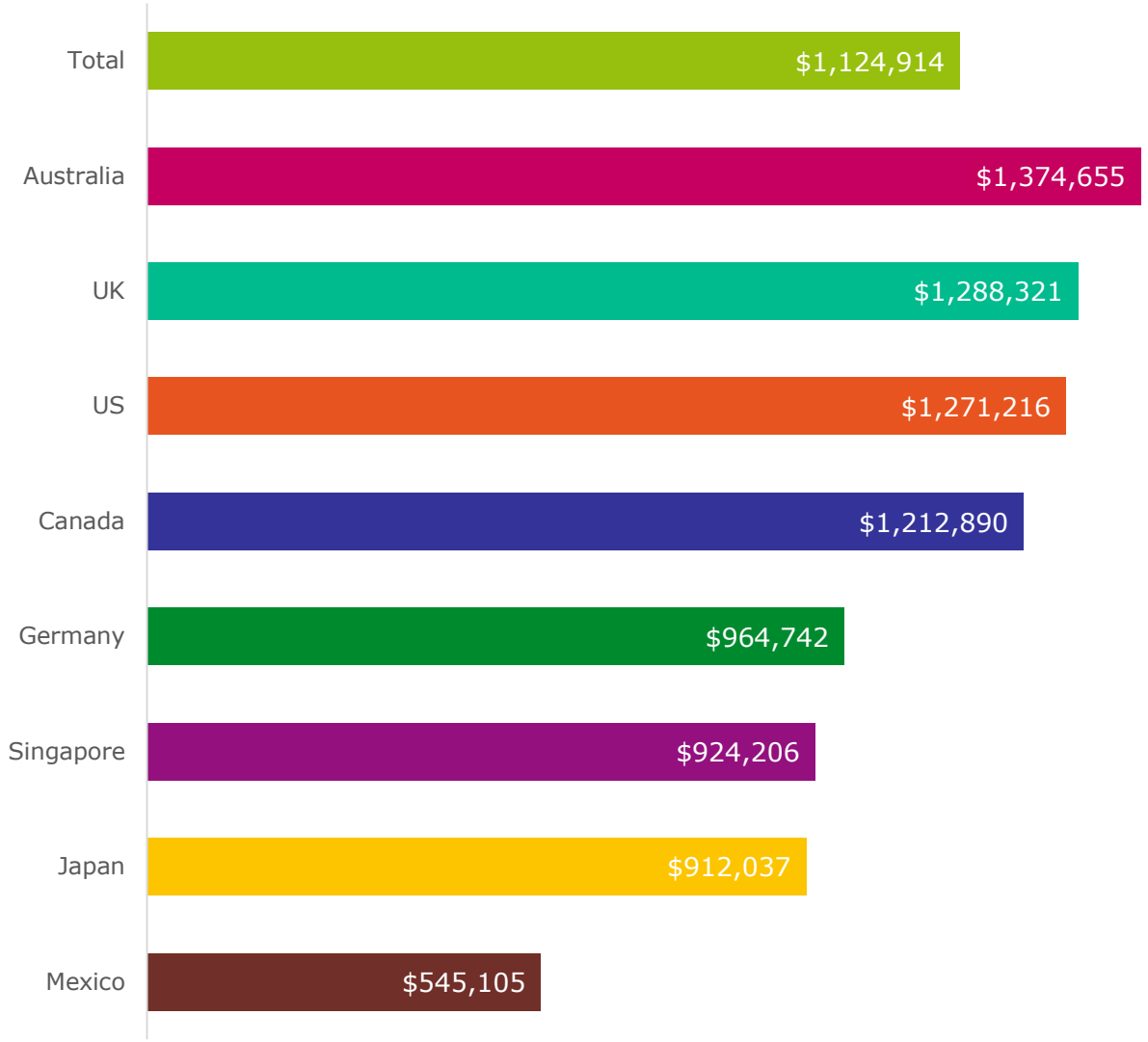


Figure 35: *Analysis showing the average cost of a software supply chain attack. Asked to respondents whose organization has experienced a software supply chain attack at some point in the past, split by organization sector, and not showing 'other commercial sector' due to a low base (860)*

VansonBourne

Cost of a software supply chain attack



Upon suffering a software supply chain attack, organizations in Australia, the UK, the US, and Canada all incurred losses exceeding $1 million, on average

Figure 36: *Analysis showing the average cost of a software supply chain attack. Asked to respondents whose organization has experienced a software supply chain attack at some point in the past, split by respondent country (860)*

VansonBourne