IBM Security Incident Responder Study

–

July 6-13, 2022

MORNING CONSULT®

IBM

KEY FINDINGS

1. Cybersecurity Incident Responders **said that the sense of duty to help and protect others/businesses was by far the most influential factor attracting them to the profession**. Continuous opportunity to learn and being rooted in problem solving followed as most influential factors.
2. **At the same time, "sense of responsibility toward their team/client"** and "**managing stakeholder expectations"** were ranked as the **most stressful aspects of responding to cyber incidents** – around half selected these amongst their top 3 stressors.
3. **The average incident response engagement is 2-4 weeks** according to 48% of respondents. And **nearly 30% say an incident response engagement lasts more than 4 weeks** on average. The overwhelming majority states it's common to be assigned to respond to two or more incidents that overlap.
4. **The first three days of responding to an attack are seen as the most stressful.** Additionally, more than a third say they are working more than 12 hours a day during the most stressful period of the engagement.
5. The majority of Cybersecurity Incident Responders think **the rise of ransomware has exacerbated the stress/psychological demands** required during a cybersecurity incident response, with 81% overall reporting this sentiment.
6. **Sixty-seven percent** of Cybersecurity Incident Responders said they **experience stress/anxiety in their daily lives as a result of responding to an incident**.
7. **Nearly 65%** of Cybersecurity Incident Responders have **sought mental health assistance as a result of responding to cybersecurity incidents**. The majority of respondents (84%) also say they have access to adequate mental health support resources.

Methodology: This study was conducted by Morning Consult on behalf of IBM from July 6-13, 2022. The study was conducted among a sample of 1,107 Cybersecurity Incident Respondents across global markets in the US, UK, Germany, Canada, Australia, France, Spain, Brazil, Japan, and India. The interviews were conducted online, and the margin of error is +/- 3 percentage points for Cybersecurity Incident Responders across global markets at a 95% confidence level.

AGENDA

CYBERSECURITY INCIDENT RESPONDER GENERAL PERCEPTIONS

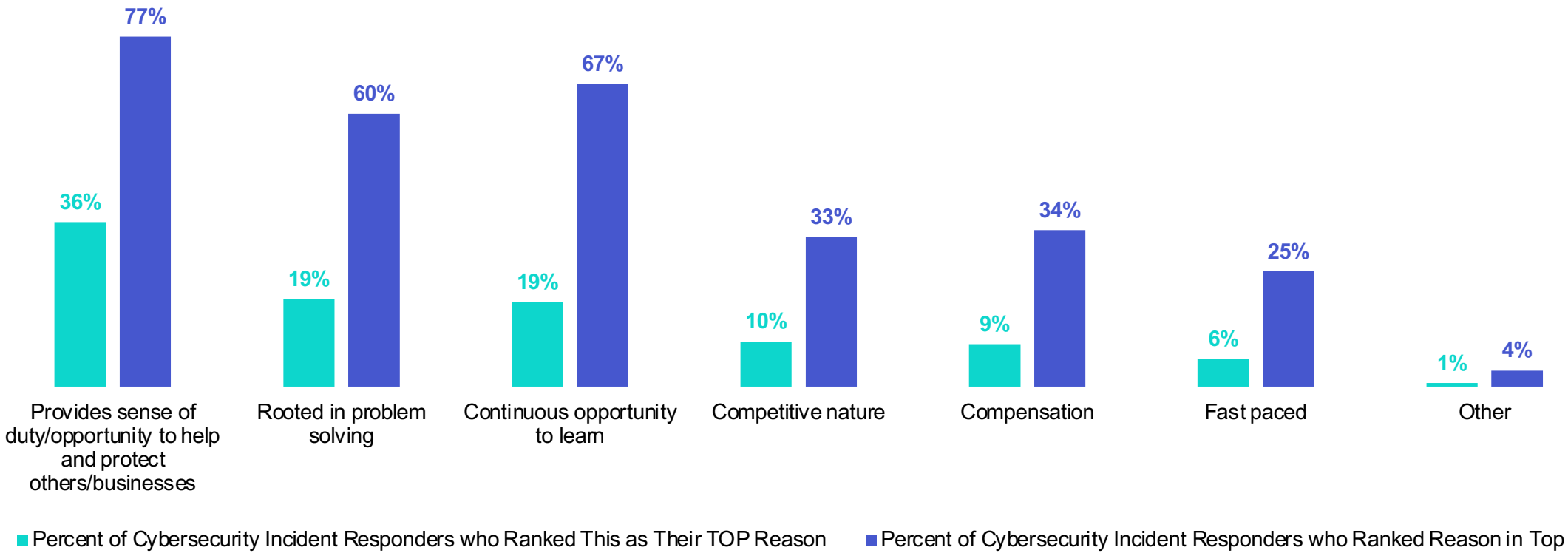
STRESSORS OF CYBERSECURITY INCIDENT RESPONSE

IMPACT ON MENTAL HEALTH & WELL BEING

MORNING CONSULT

Cybersecurity Incident Responders said that the sense of duty/opportunity to help and protect others/businesses, continuous opportunity to learn, and being rooted in problem solving were the most influential factors attracting them to the profession

Which of the following reasons attracted you to the cybersecurity incident response profession? Please drag and drop your top three in order of priority.



MORNING CONSULT

The sense of duty/opportunity to help and protect others/businesses was most influential in attracting Cybersecurity Incident Responders across markets, but problem solving was also influential for Cybersecurity Incident Responders, particularly in Spain and Japan

Which of the following reasons attracted you to the cybersecurity incident response profession? Please drag and drop your top three in order of priority.
[Showing % who ranked this as their TOP reason]

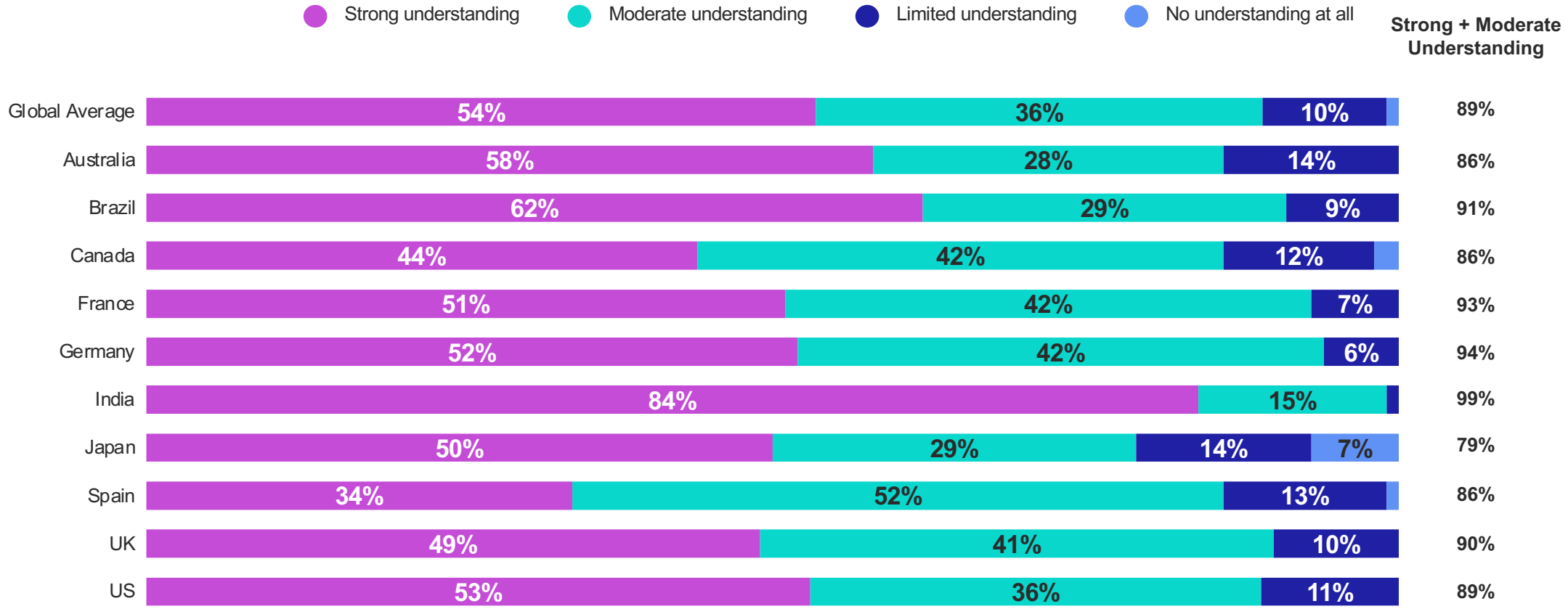
	US	UK	Germany	Canada	Australia	France	Spain	Brazil	Japan	India
Rooted in problem solving	15	15	17	19	20	19	31	16	29	13
Fast paced	5	10	5	4	9	4		11	5	8
Competitive nature	11	10	12	10	6	15	9	4	8	11
Provides sense of duty/opportunity to help and protect others/businesses	39	36	40	34	38	40	31	30	34	37
Continuous opportunity to learn	19	21	15	19	19	13	23	21	15	23
Compensation	11	7	9	13	8	8	5	16	7	8

Responses < 3% have been excluded

MORNING CONSULT

Across most markets, over half of Cybersecurity Incident Respondents think senior leadership has a strong understanding of the activities involved in Incident Response, except in Canada, Spain, and the UK

In your experience, how much of an understanding do you think senior leadership (including your employer and/or client leadership) has of the activities are involved in Incident Response?

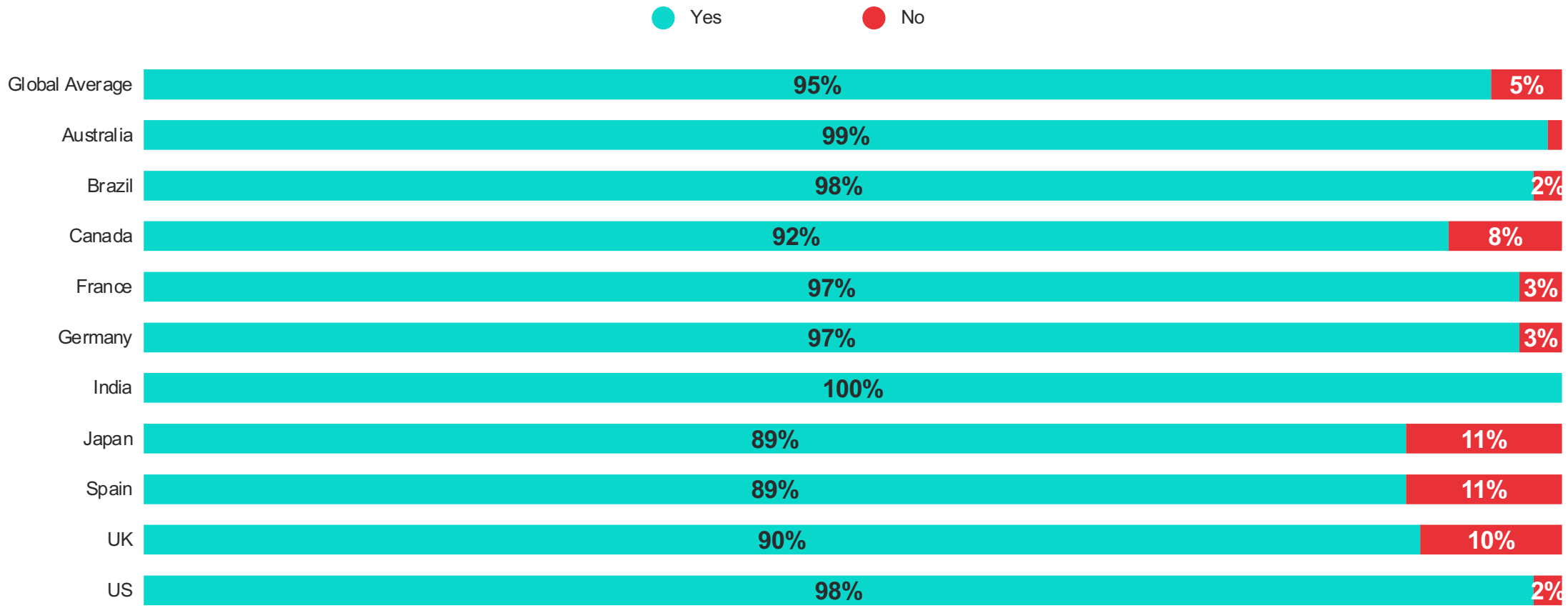


"Global Average" reflects the combined responses of Cybersecurity Incident Respondents across global markets in the US, UK, Germany, Canada, Australia, France, Spain, Brazil, Japan, and India.

MORNING CONSULT

The majority of Cybersecurity Incident Responders across markets think that senior leadership provides the necessary support structure for them to be successful (95%)

Do you think senior leadership (including your employer and/or client leadership) provides the necessary support structure for you to be successful (e.g., staffing, tools, response plans)?



AGENDA

GENERAL SENTIMENT AROUND BEING CYBERSECURITY INCIDENT RESPONDER

STRESSORS OF CYBERSECURITY INCIDENT RESPONSE

IMPACT ON MENTAL HEALTH & WELL BEING

MORNING CONSULT

Managing expectations from multiple stakeholders and the sense of responsibility toward their team/client to mitigate the incident are seen as the most stressful aspects of responding to a cybersecurity incident

Which of the following do you think are the most stressful aspects of responding to a cybersecurity incident? Please drag and drop your top three in order of priority.

MORNING CONSULT

The sense of responsibility towards their team/client to mitigate the incident is seen as the most stressful aspect of responding to a cybersecurity incident by Cybersecurity Incident Responders in Canada, Spain, and India

Which of the following do you think are the most stressful aspects of responding to a cybersecurity incident? Please drag and drop your top three in order of priority. **[Showing % who ranked this as their TOP stressor]**

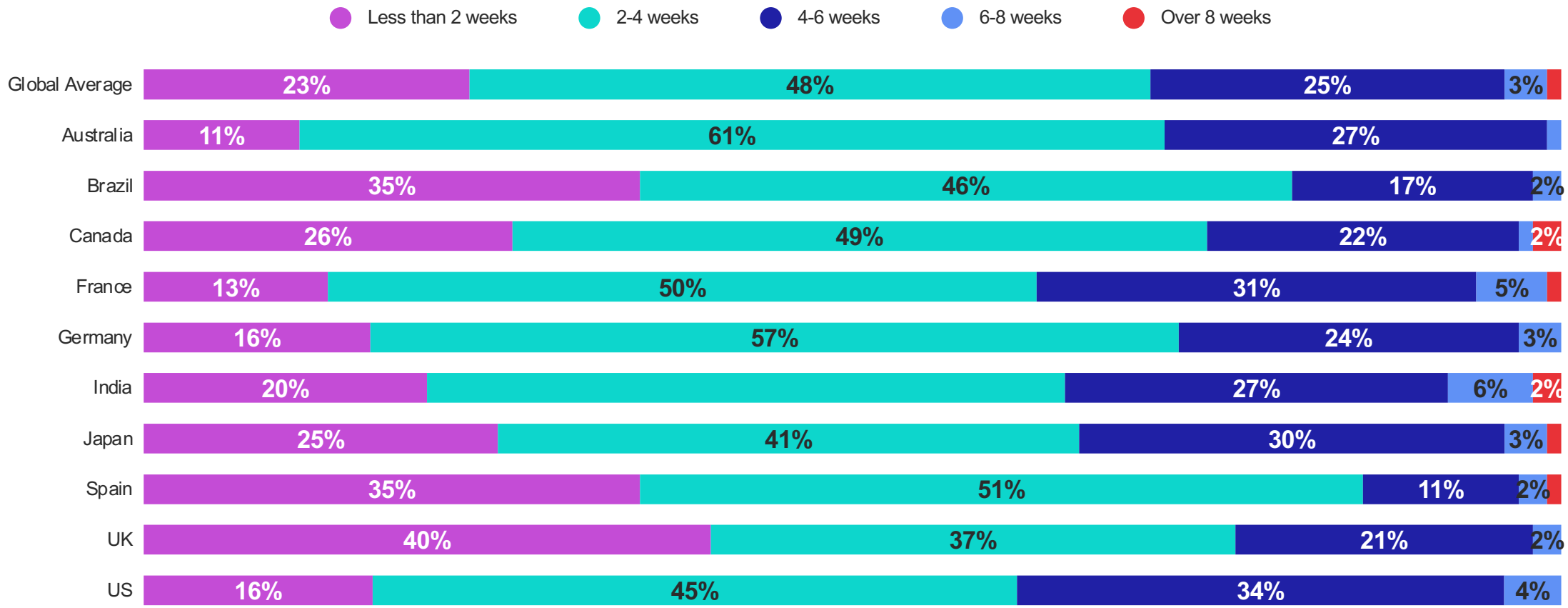
	US	UK	Germany	Canada	Australia	France	Spain	Brazil	Japan	India
The fear of missing something and/or the fear of getting something wrong	19	19	18	16	13	15	13	15	10	4
Sense of responsibility toward your team/client to mitigate the incident	15	15	14	23	16	19	23	14	16	26
Ineffective or unclear communication with client team or CISO	15	10	11	7	16	10	7	13	11	7
Pushback on recommended response/remediation approach from organization/client	14	14	17	17	26	17	4	20	18	10
Managing expectations from multiple stakeholders (e.g., pressure from C-Suite/board)	16	20	18	12	14	16	20	21	20	17
The need to act quickly	10	14	14	13	8	9	19	8	12	16
Lack of downtime/rest	4	3	3	5	4	3	3			7

Responses < 3% have been excluded

MORNING CONSULT

On average, 71% have an incident response engagement of 4 weeks or less; 39% of US Cybersecurity Incident Responders have an average incident response engagement of more than 4 weeks

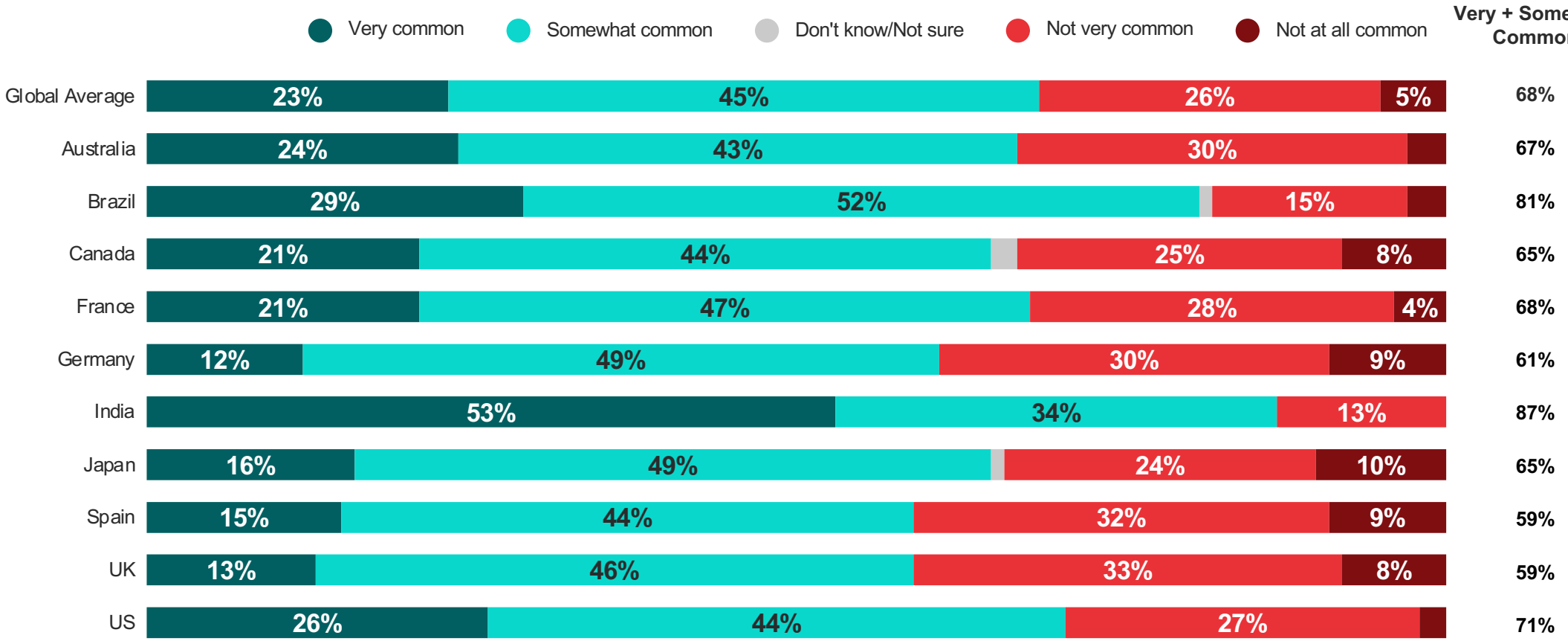
For the incidents that you have responded to, what is the average length of an incident response engagement?



MORNING CONSULT

A majority (68%) say that it is very or somewhat common for them to be assigned to respond to two or more cybersecurity incidents that overlap

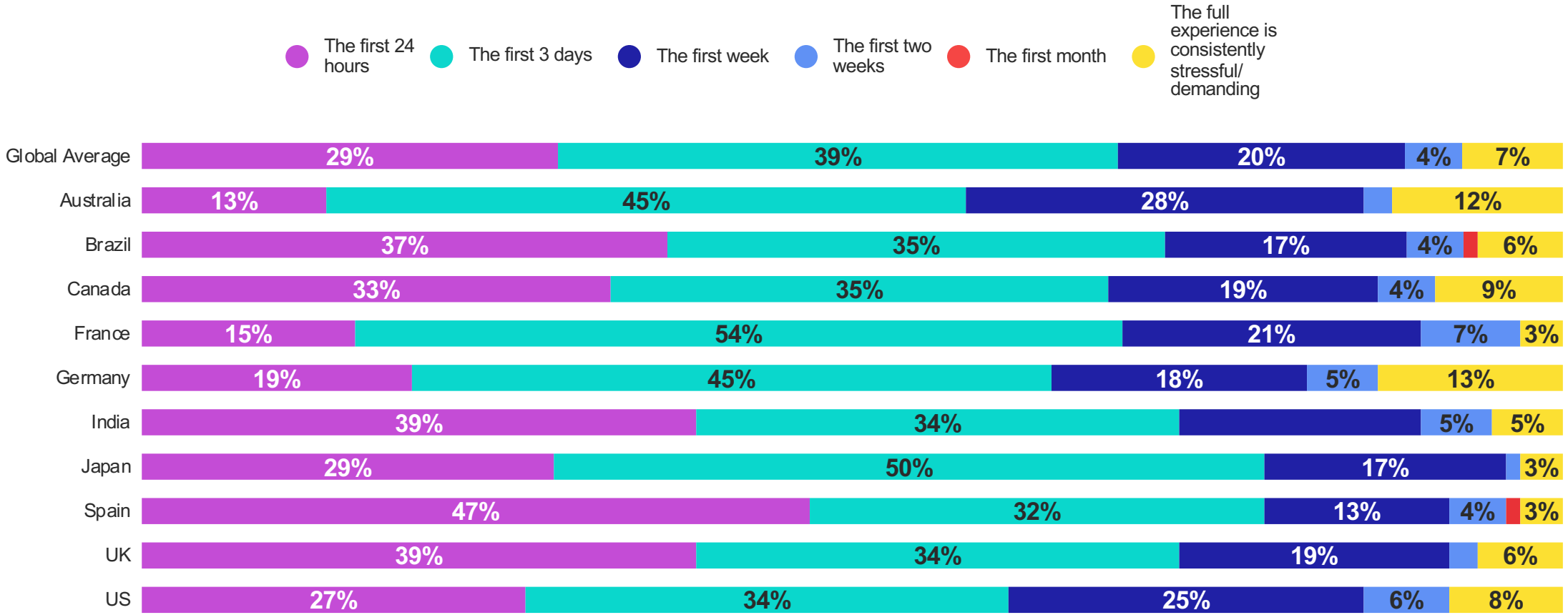
In your experience, how common is it to be assigned to respond to two or more cybersecurity incidents that overlap?



MORNING CONSULT

39% say the first 3 days is the most stressful/demanding when responding to a cybersecurity incident

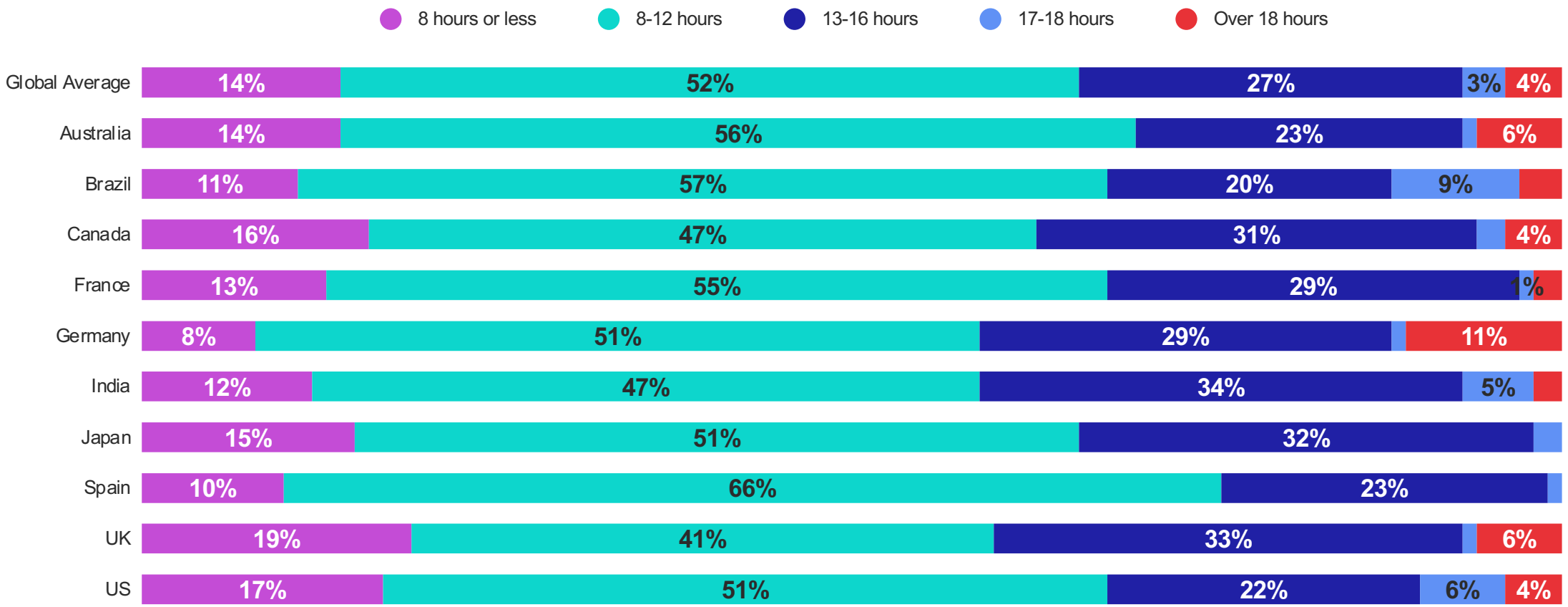
When responding to a cybersecurity incident, which period do you consider to be the most stressful/demanding?



MORNING CONSULT

More than a third say they are working more than 12 hours a day during the most stressful period of the engagement

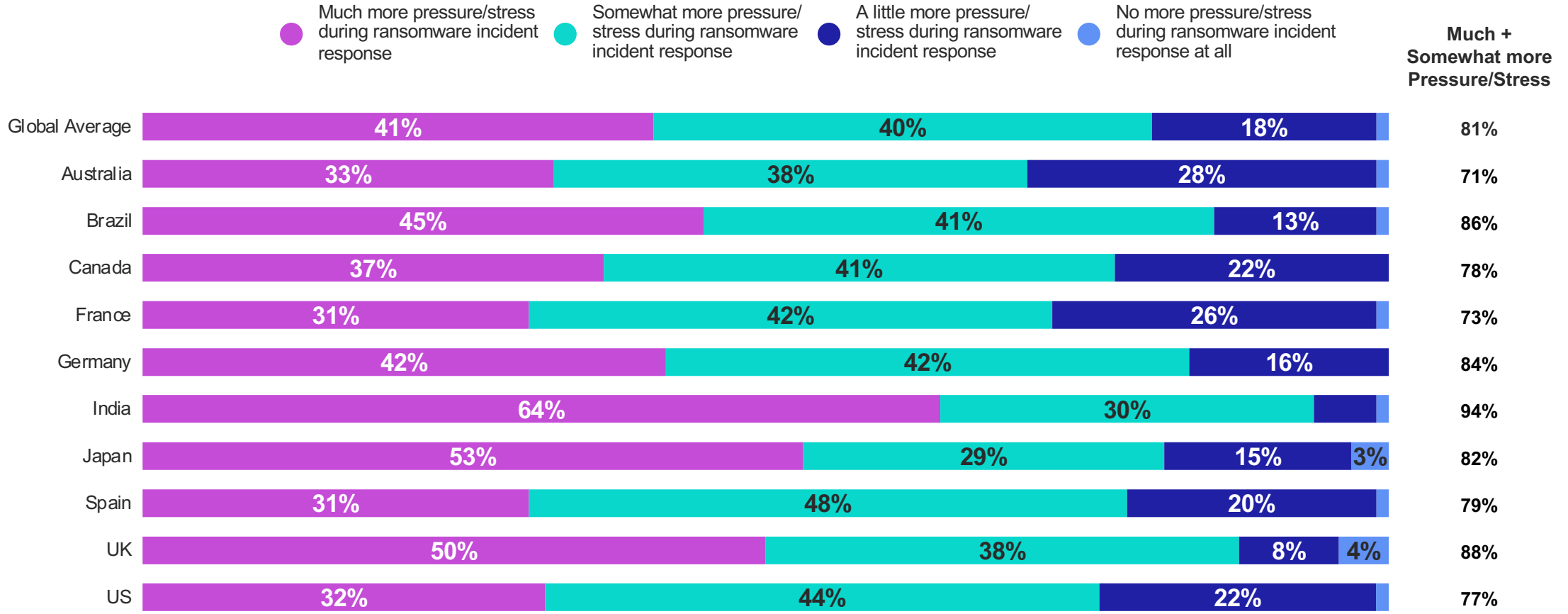
On average, when responding to a cybersecurity incident, how many hours per day do you work during that most stressful period of the engagement?



MORNING CONSULT

A majority of Cybersecurity Incident Responders across markets think the rise of ransomware has exacerbated the stress/psychological demands required during a cybersecurity incident response, with 81% overall reporting this sentiment

To what extent do you think the rise of ransomware attacks has exacerbated the stress/psychological demands required during a cybersecurity incident response?



AGENDA

GENERAL SENTIMENT AROUND BEING CYBERSECURITY INCIDENT RESPONDER

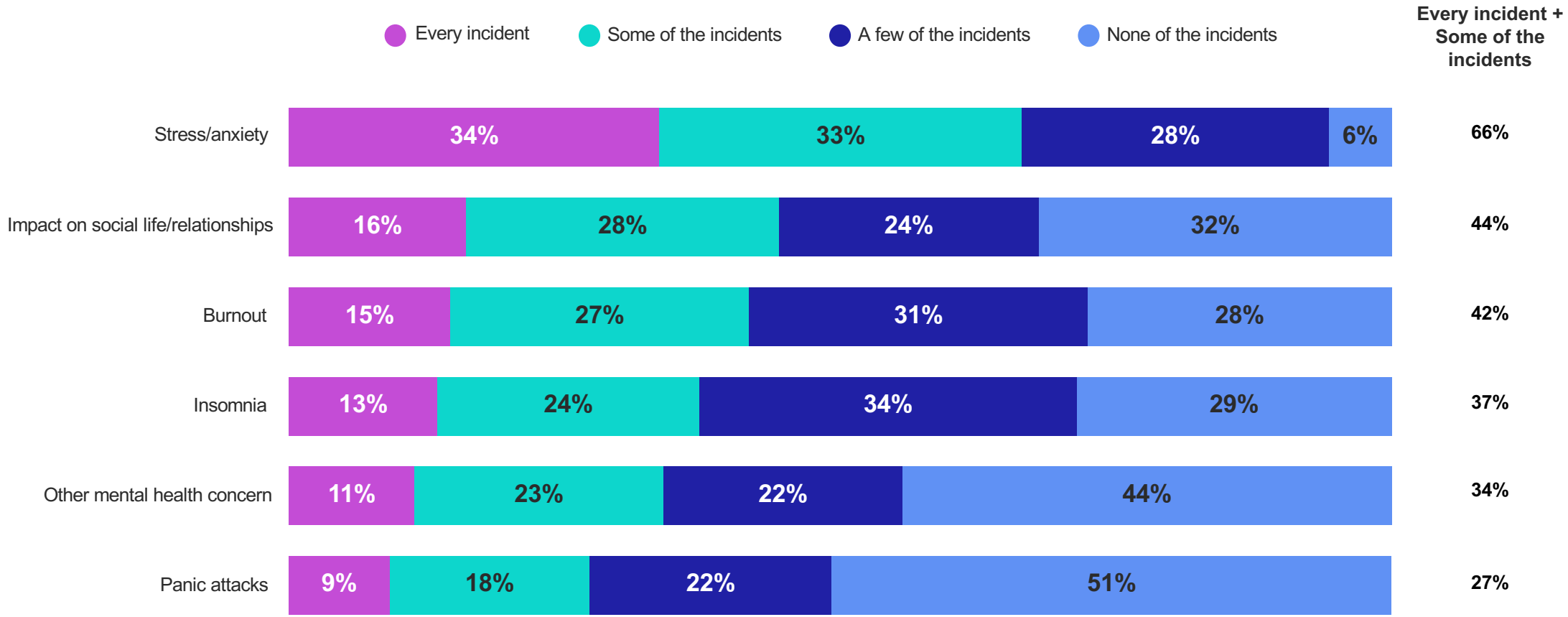
STRESSORS OF CYBERSECURITY INCIDENT RESPONSE

IMPACT ON MENTAL HEALTH & WELL BEING

MORNING CONSULT

Stress/anxiety are the most common sentiments/conditions among Cybersecurity Incident Responders while responding to an incident (66%), but over 40% report there being an impact on their social life/relationships (44%) and burnout (42%) from responding to a cybersecurity incident

How frequently have you experienced the following sentiments/conditions while responding to a cybersecurity incident?



MORNING CONSULT

Across all countries, stress/anxiety are the most common sentiments/conditions while responding to a cybersecurity incident

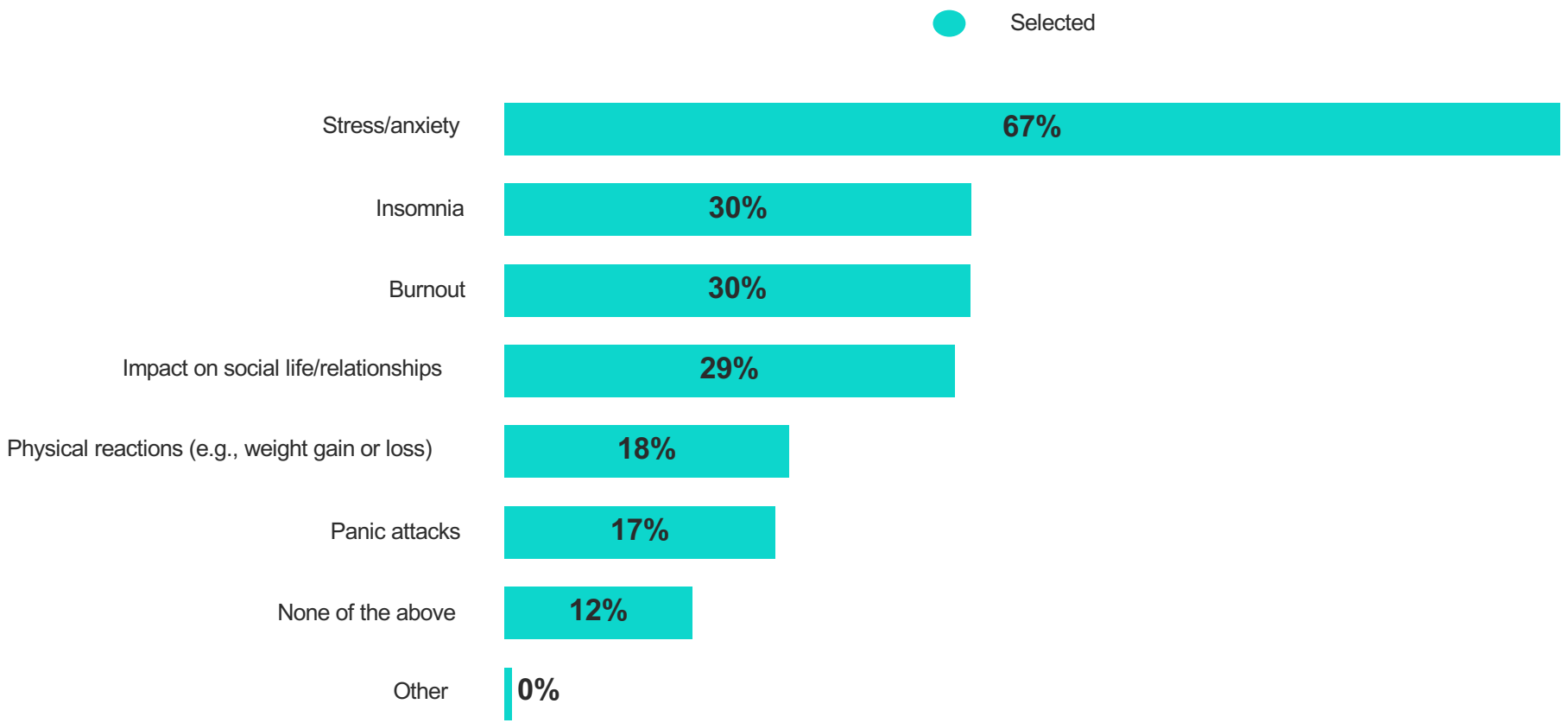
How frequently have you experienced the following sentiments/conditions while responding to a cybersecurity incident? **[Showing % Every incident + Some of the incidents]**

	US	UK	Germany	Canada	Australia	France	Spain	Brazil	Japan	India
Burnout	35	45	23	47	24	21	69	59	46	56
Stress/anxiety	64	65	62	63	60	56	71	79	65	83
Panic attacks	25	22	26	30	24	23	19	32	20	55
Insomnia	34	29	34	34	22	30	48	62	33	50
Impact on social life/relationships	42	47	42	44	30	35	43	49	45	71
Other mental health concern	27	26	26	26	33	21	19	58	47	64

MORNING CONSULT

Two thirds (67%) of Cybersecurity Incident Responders have experienced stress/anxiety in their daily lives as a result of responding to cybersecurity incidents; around 30% have also experienced insomnia (30%), burnout (30%) and their social life/relationships have been impacted (29%)

Have you experienced any of the following in your daily life as a result of responding to cybersecurity incidents? Select all that apply. **[Showing % Selected]**



MORNING CONSULT

Cybersecurity Incident Responders in the UK, Spain, and Brazil are more likely to have experienced stress/anxiety in their daily lives as a result of responding to cybersecurity incidents; Cybersecurity Incident Responders in Spain also report experiencing burnout more than those in other countries

Have you experienced any of the following in your daily life as a result of responding to cybersecurity incidents? Select all that apply. **[Showing % Selected]**

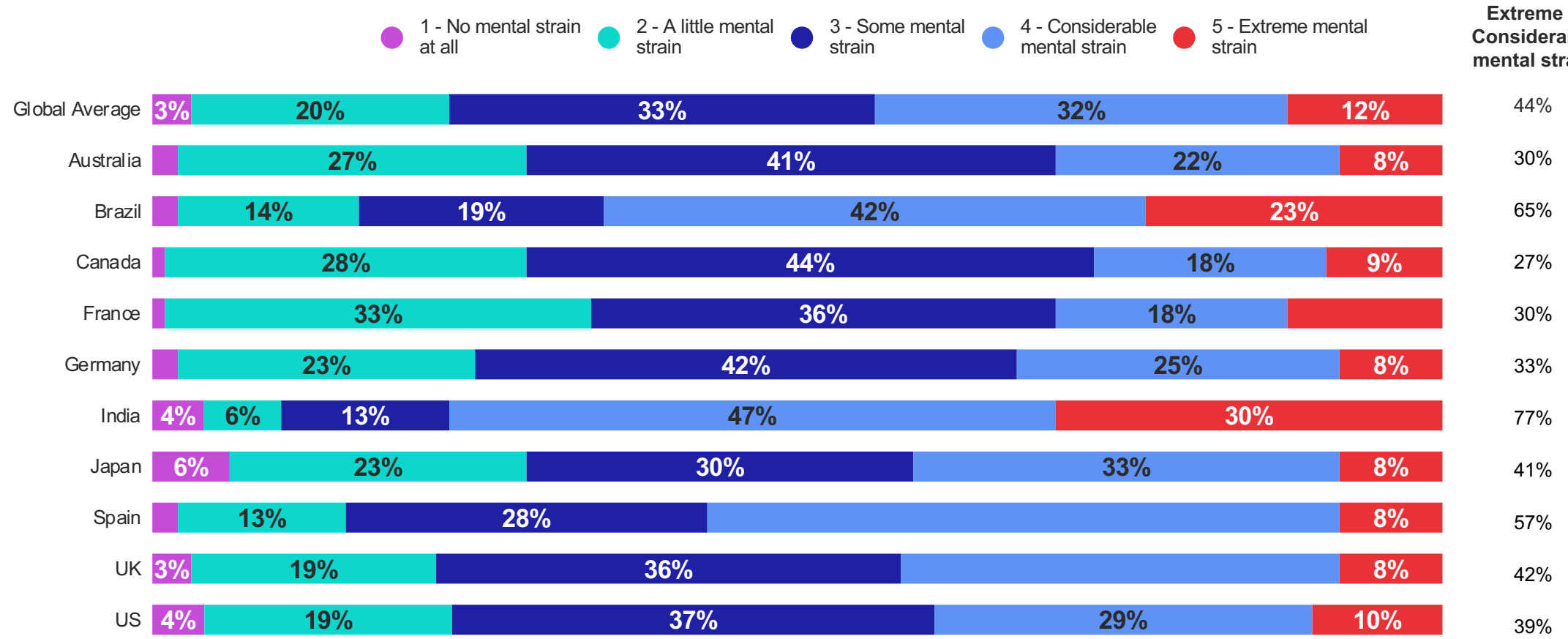
	US	UK	Germany	Canada	Australia	France	Spain	Brazil	Japan	India
Burnout	27	38	20	34	11	21	52	34	26	35
Stress/anxiety	61	78	69	63	50	64	74	84	65	68
Panic attacks	17	17	6	16	9	18	16	22	9	41
Insomnia	20	20	36	24	14	36	42	60	20	34
Impact on social life/relationships	30	35	28	21	14	23	31	34	17	51
Physical reactions (e.g., weight gain or loss)	16	12	15	15	16	10	16	28	20	34
None of the above	10	7	6	18	31	13	8	3	13	

Responses < 3% have been excluded

MORNING CONSULT

Over 40% of Cybersecurity Incident Responders say they have experienced extreme or considerable mental strain as a result of responding to a major cybersecurity incident, with those in Brazil (65%), India (77%), and Spain (57%) more likely to express this sentiment

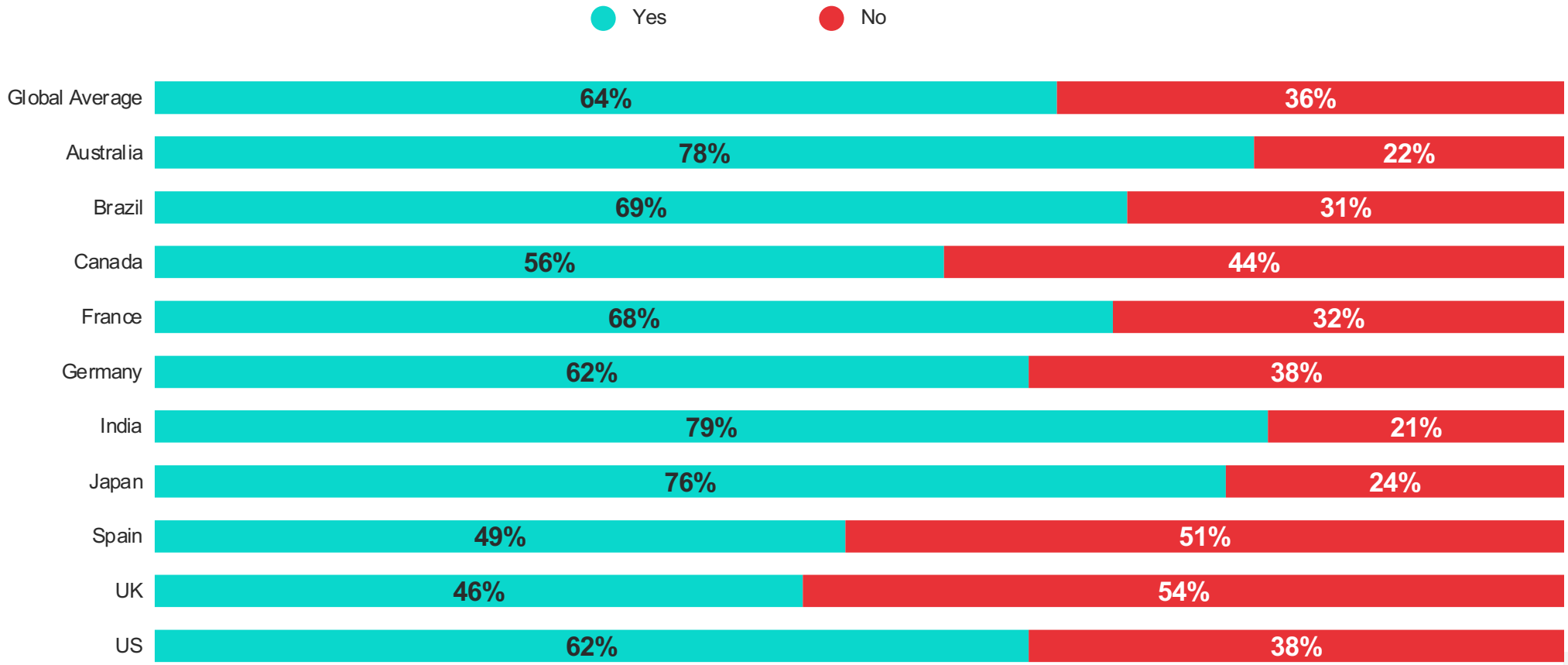
How would you rank the mental strain of responding to a major cybersecurity incident (e.g., WannaCry (2017), NotPetya (2017), SolarWinds (2021), Kaseya (2022)) on scale of 1 to 5, where 1 is little to no toll and 5 is extreme mental toll?



MORNING CONSULT

64% have sought mental health assistance as a result of responding to cybersecurity incidents, with those Australia (78%), India (79%), and Japan (76%) more likely to say they sought mental health assistance than responders in other countries

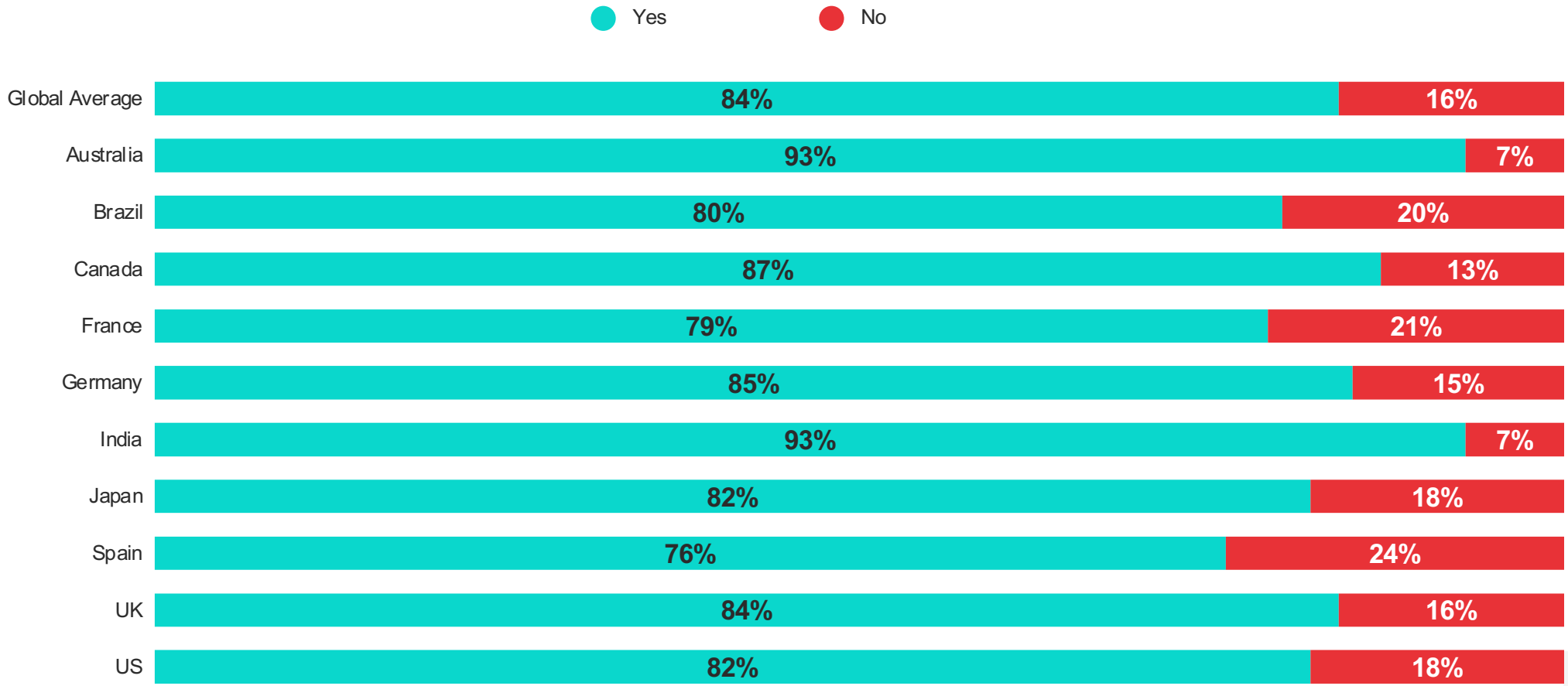
Have you sought mental health assistance as a result of responding to cybersecurity incidents?



MORNING CONSULT

A majority of Cybersecurity Incident Responders say that they have adequate access to mental health support resources, with 84% overall saying so

Do you feel you have access to adequate mental health support resources?



Steps businesses can take to help Incident Responders be successful

Incident Responders are tasked with defending constantly expanding environments from evolving and increasingly aggressive threats. While there's an innate sense of urgency that comes with the territory, steps businesses take to prepare for a cyber crisis can make all the difference in achieving speedy, cost-efficient response and recovery, alleviating unnecessary pressure for their Incident Responders. Here are two key steps that can help businesses enhance their cyber preparedness and incident response effectiveness:

1. **Create Detailed Incident Response Plans and Playbooks:** It's important to develop plans and playbooks that are customized to each business's environment, technologies, and resources. This enables businesses to account in advance for the resources required in the event of a security incident, establish those contacts as well as have an Incident Response retainer subscription that will make incident response services readily available to them during a cyber crisis.

2. **Rehearse and Test Your Incident Response Under Pressure**: It's not a matter of if an organization's security team will be tested by a cyberattack anymore, but a matter of when. By conducting simulation exercises the organization and security team can feel what it's like to respond under pressure and identify their gaps and areas or processes they need to improve in order to effectively activate in the event of a real-life security event. This includes ensuring external security teams are correctly integrated into their response team.

Additional Resources

– Register for IBM Security's Incident Responder webinar on October 12, 2022, at 1:00 pm ET

– Schedule an IBM Security X-Force consultation

– Learn more about an IBM Security X-Force incident response subscription with IBM Security X-Force