PULSE Hitachi ID

Employees from Nearly 50% of Businesses Have Been Approached to Assist in Ransomware Attacks, Hitachi ID Survey Reveals

Ransomware attacks are plaguing organizations, and they are becoming increasingly disruptive and sophisticated. Gasoline suppliers, higher education institutions, insurance companies and even the Houston Rockets fell victim to ransomware this year. And these attacks aren't just coming from the outside. Nearly 50% of employees and leaders have been approached to assist in ransomware attacks — emphasizing the need for businesses of all shapes and sizes to take a proactive security offence to cybersecurity.

One solution is to implement a zero-trust model to mitigate ransomware attacks and protect an organization's most valuable resources. As digital transformations continue, what are organizations doing to protect themselves?

Pulse and Hitachi ID surveyed 100 IT and security executives to understand what changes are being made to cybersecurity infrastructure, how those changes are able to handle cyberattacks, and how politics plays a role.

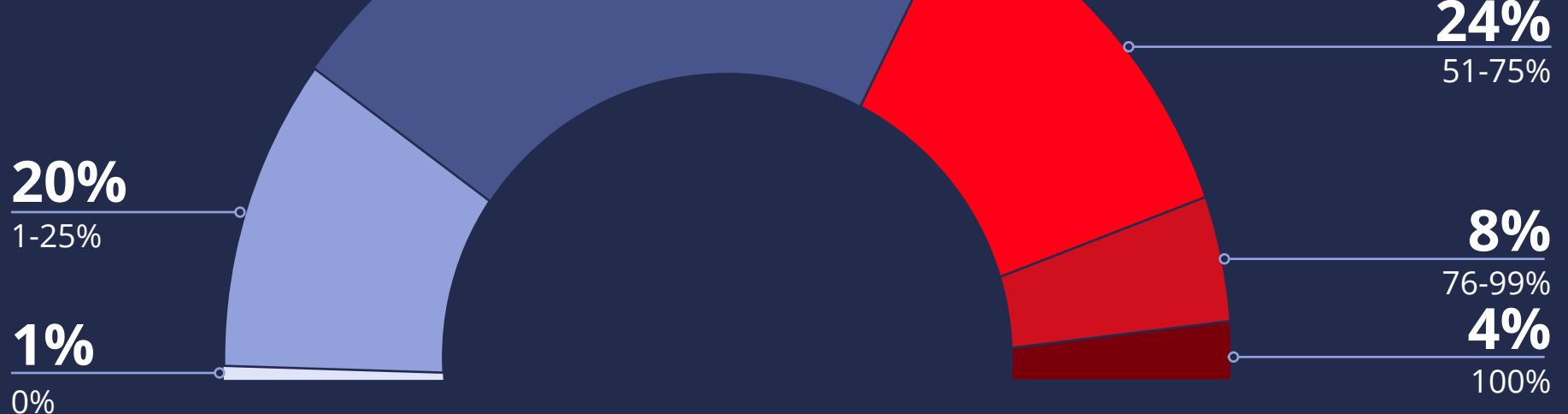
Data collected from September 1 - September 23, 2021

Respondents: 100 IT and security executives

ALMOST ALL ARE MOVING SOME OF THEIR SECURITY-RELATED DIGITAL TRANSFORMATION TO SAAS AND MANY HAVE LEGACY SYSTEMS IN PLACE THEY ARE TRYING TO SECURE

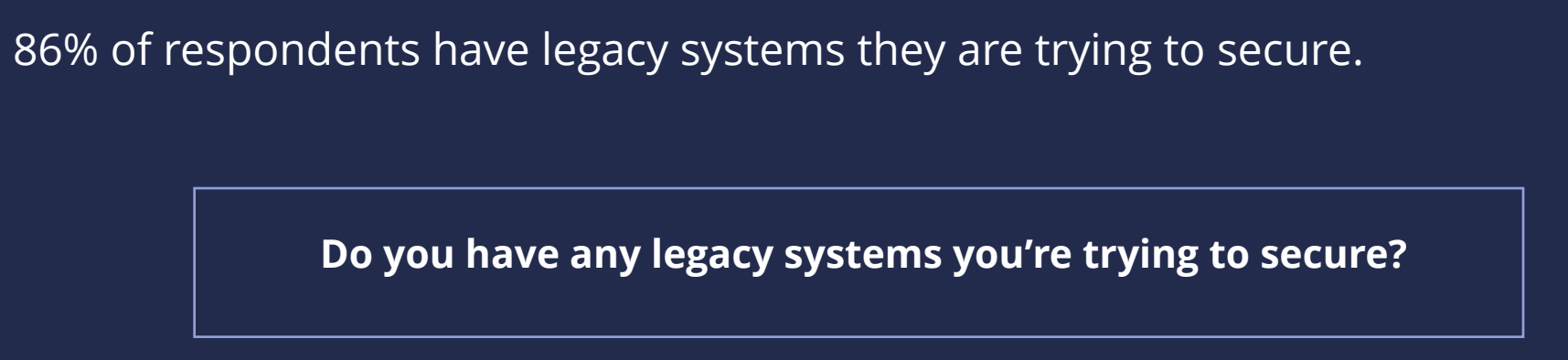
99% of executives say that at least some part of their security-related digital transformation efforts include a move to SaaS. More than a third (36%) say over half of their efforts include a move to SaaS.

How much of your security-related digital transformation efforts include a move to SaaS?



86% of respondents have legacy systems they are trying to secure.

Do you have any legacy systems you're trying to secure?



MOST ARE CONFIDENT IN THEIR CYBERSECURITY INFRASTRUCTURE TO HANDLE ATTACKS, MAINLY USING MULTI-FACTOR AUTHENTICATION AND SINGLE SIGN-ON WHILE ZERO TRUST ADOPTION IS LACKING

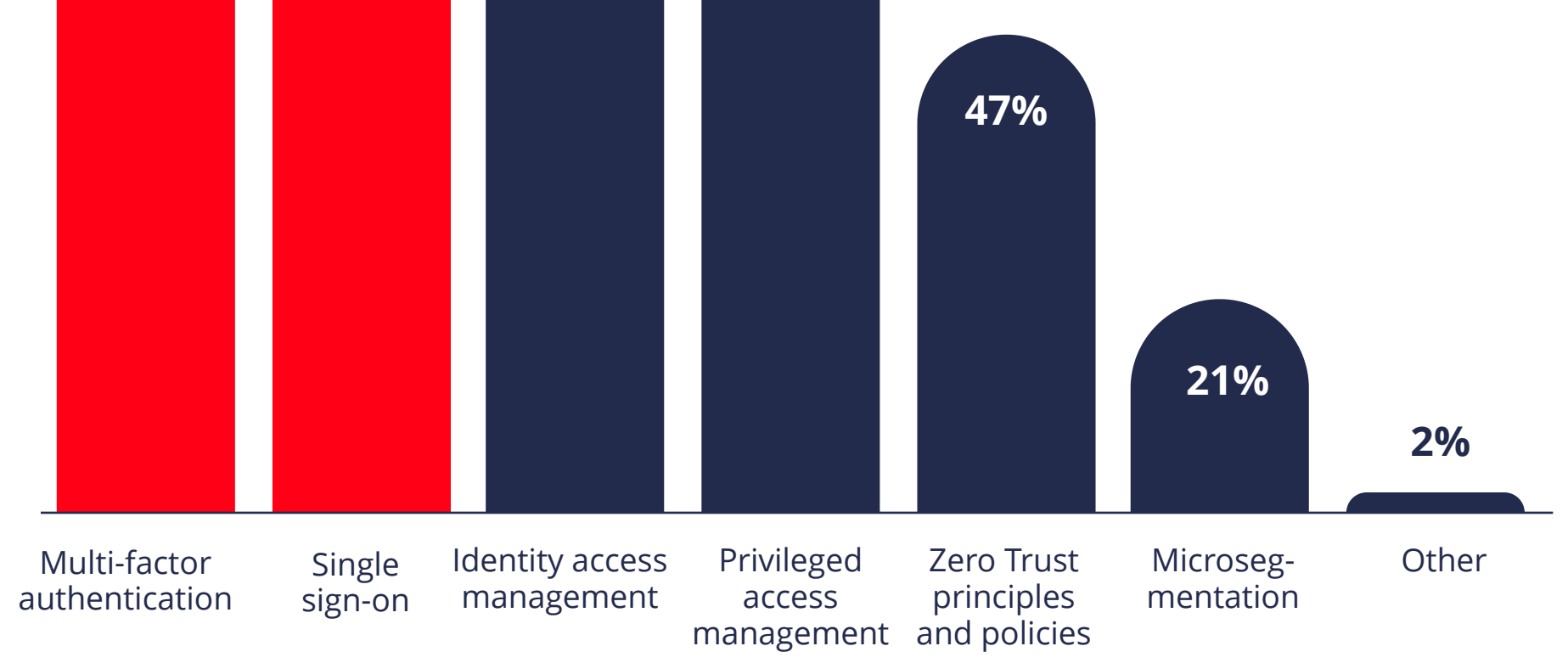
Overall, a majority (68%) of executives are moderately confident in their current cybersecurity infrastructure to protect their organization from attacks now compared to a year ago. In addition, VP's are the most confident, with 14% saying they are highly confident in their organization's current cybersecurity infrastructure.

How confident are you in your current cybersecurity infrastructure to protect your organization from attacks now vs a year ago?

	Highly confident	Moderately confident	Somewhat confident	Not confident
Overall	6%	68%	22%	4%
C-Suite	4%	78%	11%	7%
VP	14%	59%	27%	
Director	4%	67%	25%	4%

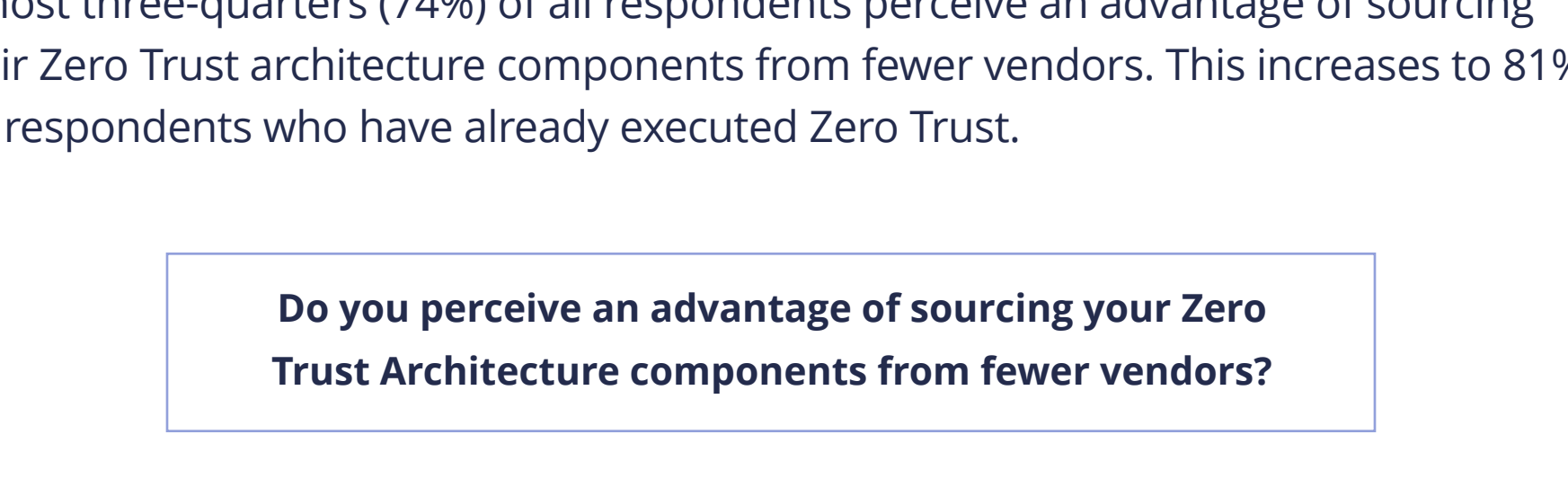
Most decision-makers have already executed multi-factor authentication (82%), single sign-on (80%), and identity access management (74%) projects.

What projects have you already executed toward your goal?



Although only 47% of respondents have executed Zero Trust principles and policies, almost three-quarters (74%) of all respondents perceive an advantage of sourcing their Zero Trust architecture components from fewer vendors. This increases to 81% for respondents who have already executed Zero Trust.

Do you perceive an advantage of sourcing your Zero Trust Architecture components from fewer vendors?



RANSOMWARE ATTACKS AREN'T JUST COMING FROM OUTSIDE THE ORGANIZATION. EMPLOYEES AND LEADERS HAVE INCREASINGLY BEEN APPROACHED TO ASSIST IN RANSOMWARE ATTACKS—AND MOST LEADERS ARE INCREASING CYBERSECURITY EDUCATION TO COPE WITH THESE HEIGHTENED RISKS

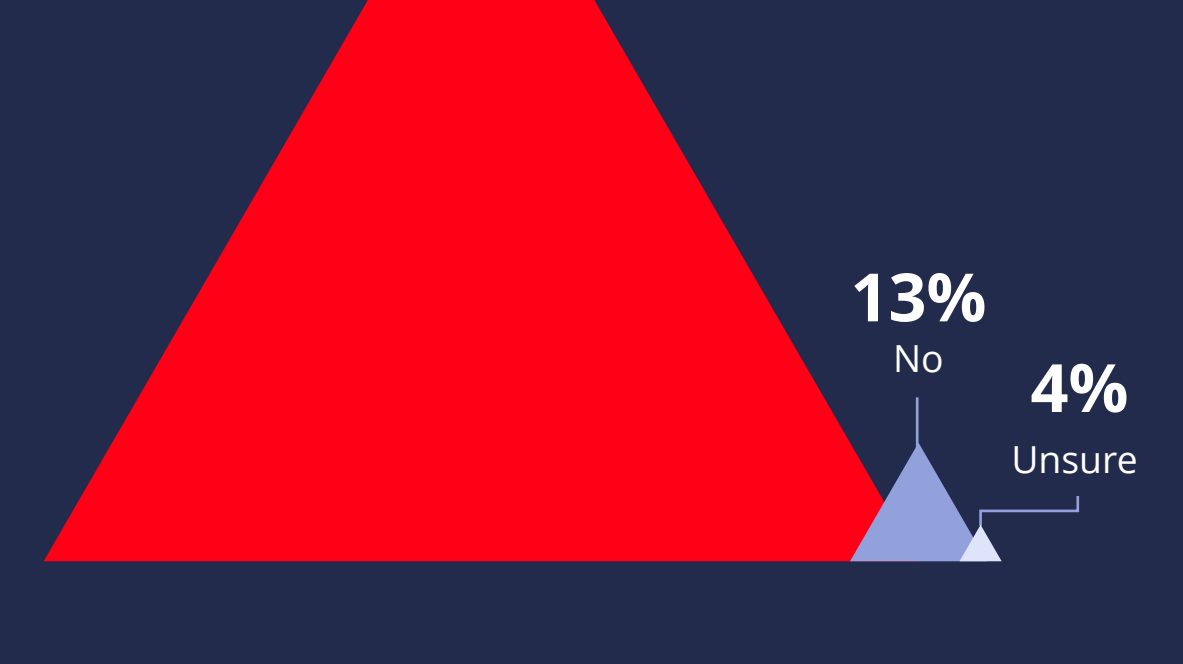
Almost half (48%) of respondents say they or their employees have been approached directly to assist in planning ransomware attacks. Interestingly, more than half (55%) of directors say they have been approached.

Have you or your employees been approached directly to assist in planning ransomware attacks?

	Yes	No	Unsure
Overall	48%	43%	9%
C-Suite	37%	63%	
VP	46%	36%	18%
Director	55%	35%	10%

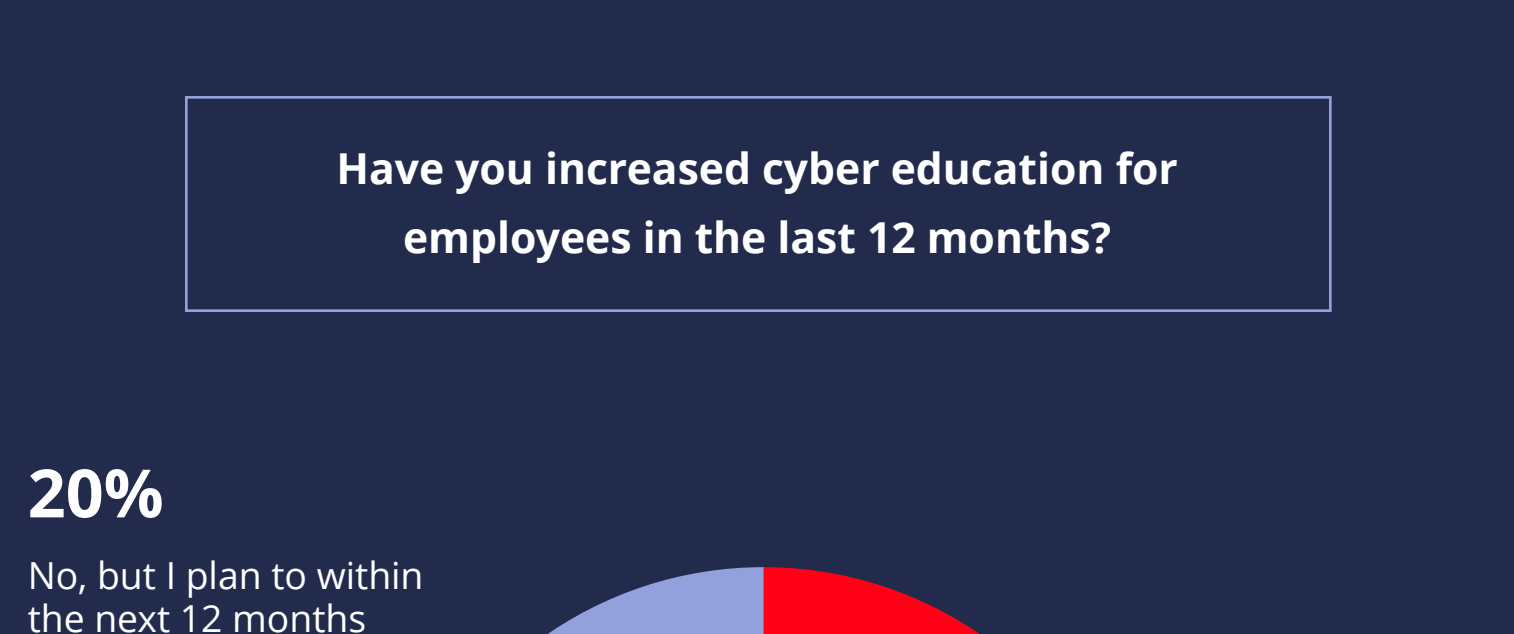
Of those who have been approached to assist in ransomware attacks, 83% of them say it has become more prominent since employees started working from home.

Has this become more prominent since employees started working remotely?



With these types of attacks that rely on insider access, educating employees on cybersecurity is paramount. 69% of executives have increased cyber education for employees in the last 12 months, and 20% have not, but plan to in the next 12 months.

Have you increased cyber education for employees in the last 12 months?



A majority of executives say that they have educated their employees on the actions they should take to prevent phishing attacks (89%), create secure passwords (86%), and keep those passwords safe (95%). Interestingly, 9% of executives are not sure if they have informed their employees about how to prevent phishing attacks.

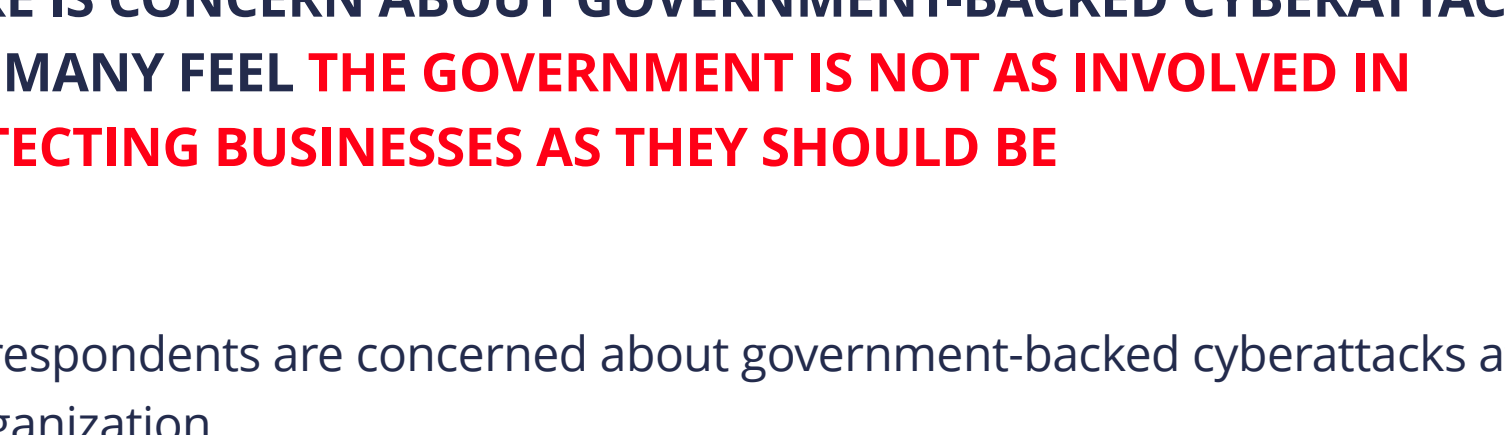
Has your organization outlined and made employees aware of specific actions they should take for the following security measures?

	Yes	No	Unsure
Prevent phishing attacks	89%	2%	9%
Create secure passwords	86%	6%	8%
Keep passwords safe	95%	2%	3%

THERE IS CONCERN ABOUT GOVERNMENT-BACKED CYBERATTACKS—AND MANY FEEL THE GOVERNMENT IS NOT AS INVOLVED IN PROTECTING BUSINESSES AS THEY SHOULD BE

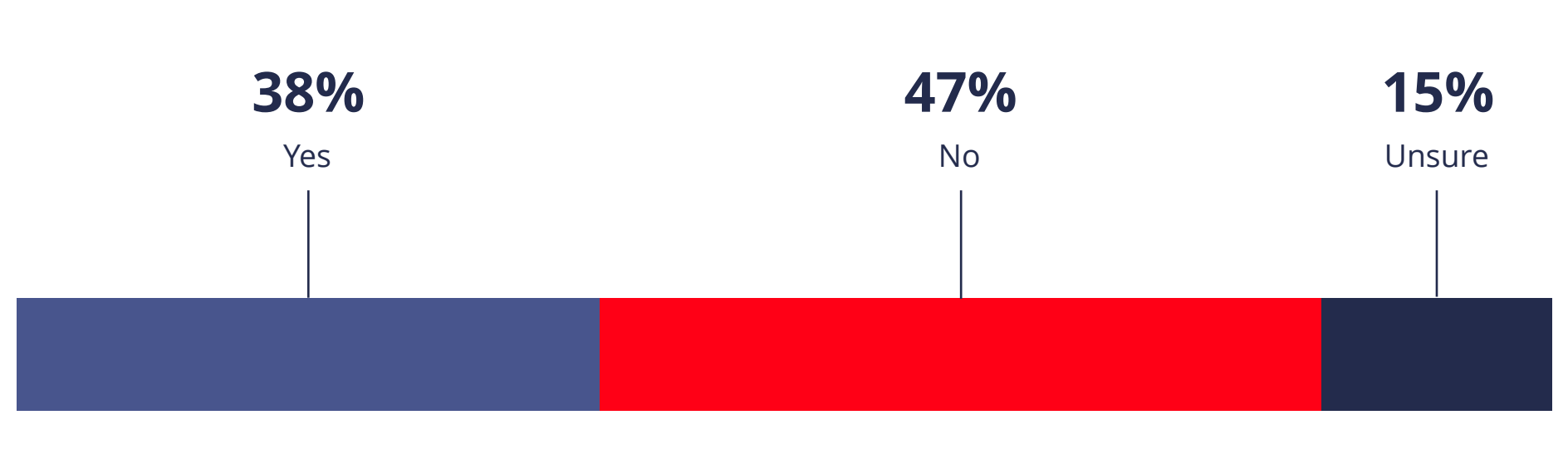
76% of respondents are concerned about government-backed cyberattacks affecting their organization.

Are you concerned about government-backed cyberattacks affecting your organization?



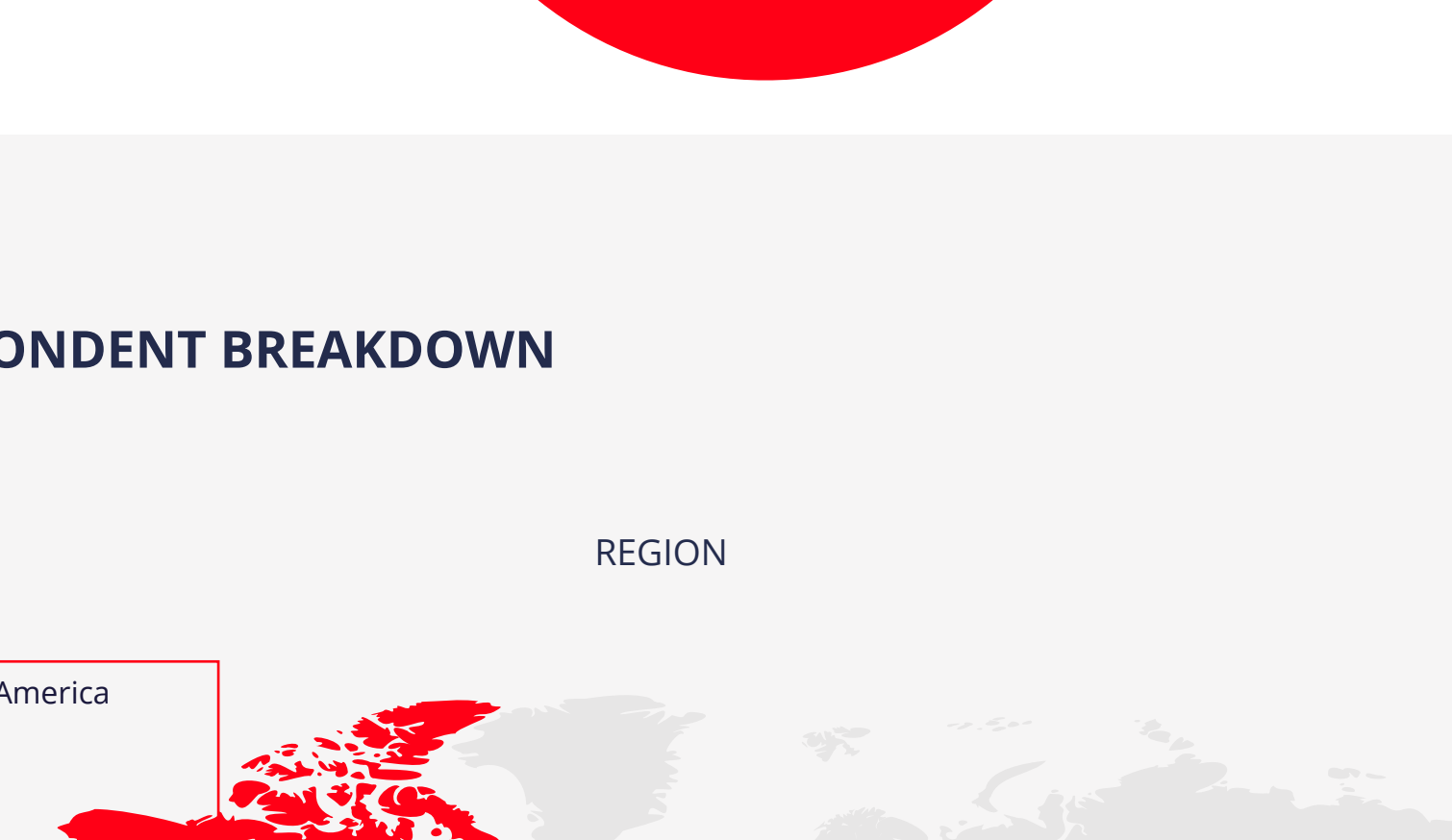
Almost half (47%) say they do not think the government is taking enough action to protect businesses from cyberattacks.

Do you think the government is taking enough action to protect businesses from cyberattacks?



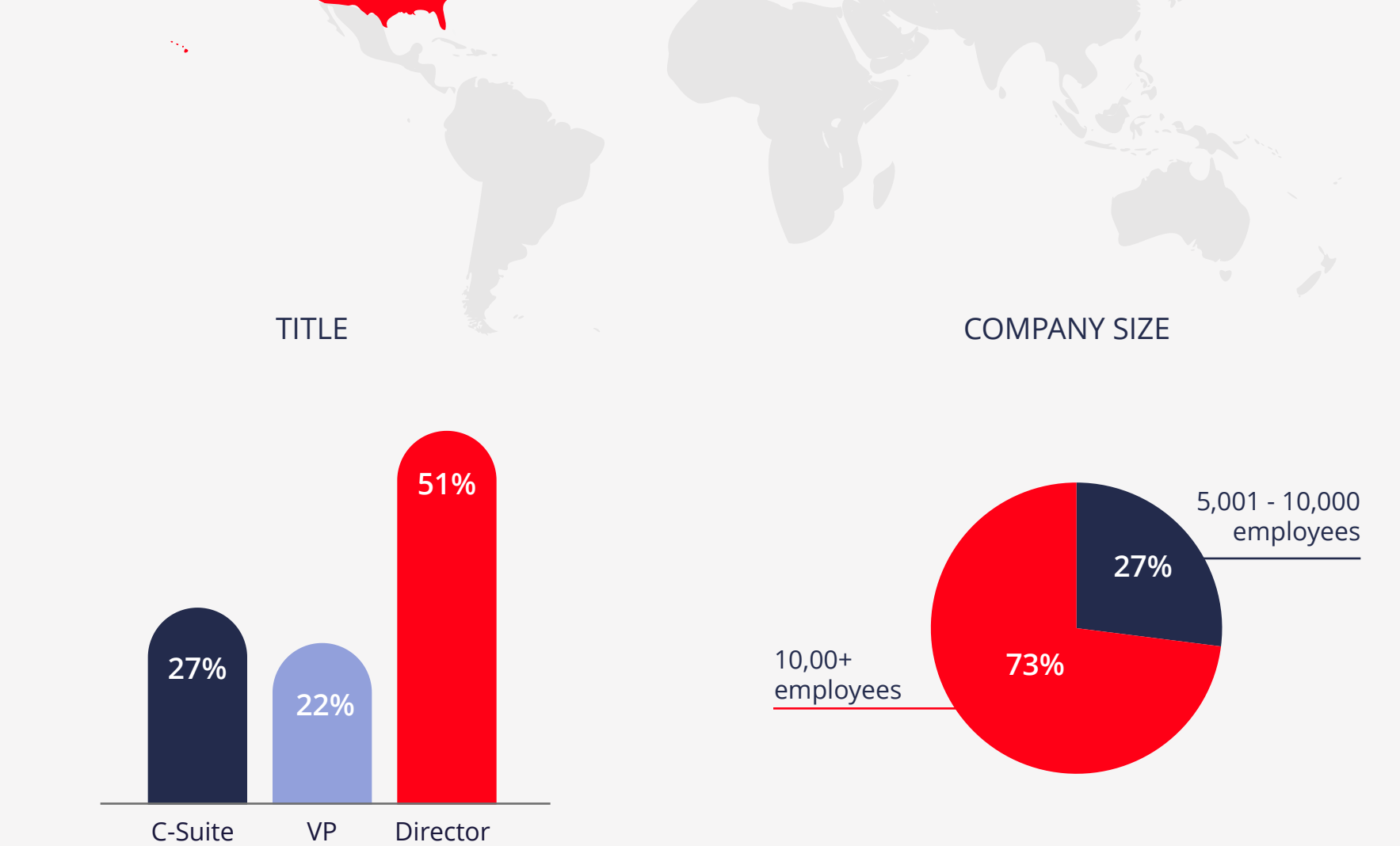
In addition, 81% of respondents think government bodies should play a larger role in defining national cybersecurity protocol and infrastructure.

Do you think government bodies should play a larger role in defining national cybersecurity protocol and infrastructure?

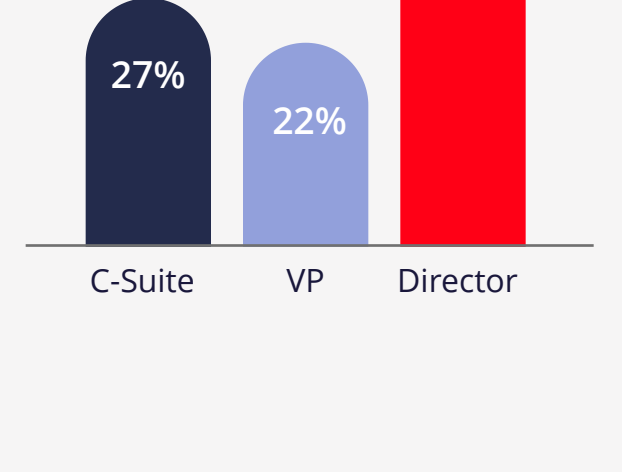


RESPONDENT BREAKDOWN

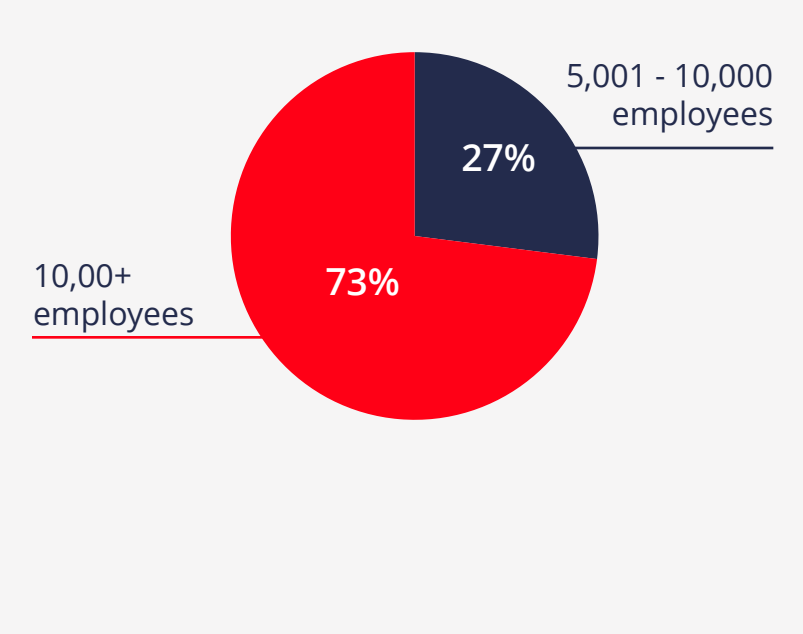
REGION



TITLE



COMPANY SIZE



Insights powered by PULSE