PULSE Lookout

US Government Response to Cybersecurity: The Tech Leaders' View

One Minute Insights:

- Most decision-makers feel somewhat informed about the US Government's cybersecurity announcements and initiatives
- Decision-makers are split over how effective the US Government's cybersecurity initiatives will be at defending both governmental infrastructure and businesses in general
- 180 days to implement cybersecurity improvements in US Government agencies is seen as a challenging timeline
- Most would target Zero Trust architecture implementation as the first undertaking that US Government agencies should act upon improving
- Legacy technology and skills gaps are seen as the top challenges to implementing a standardized approach to cybersecurity in the US, which most agree is needed
- Three times as many decision-makers believe that the tools used for malicious cybersecurity attacks are in a stronger position than the US Government's cybersecurity defences

The US Government announced several cybersecurity initiatives in 2021, including President Biden's Executive Order on Improving the Nation's Cybersecurity1. In light of such initiatives, Pulse surveyed over 150 verified technology decision-makers to gauge their opinions on the Government's response to the rising issue of ransomware and other cybersecurity attacks in the US.

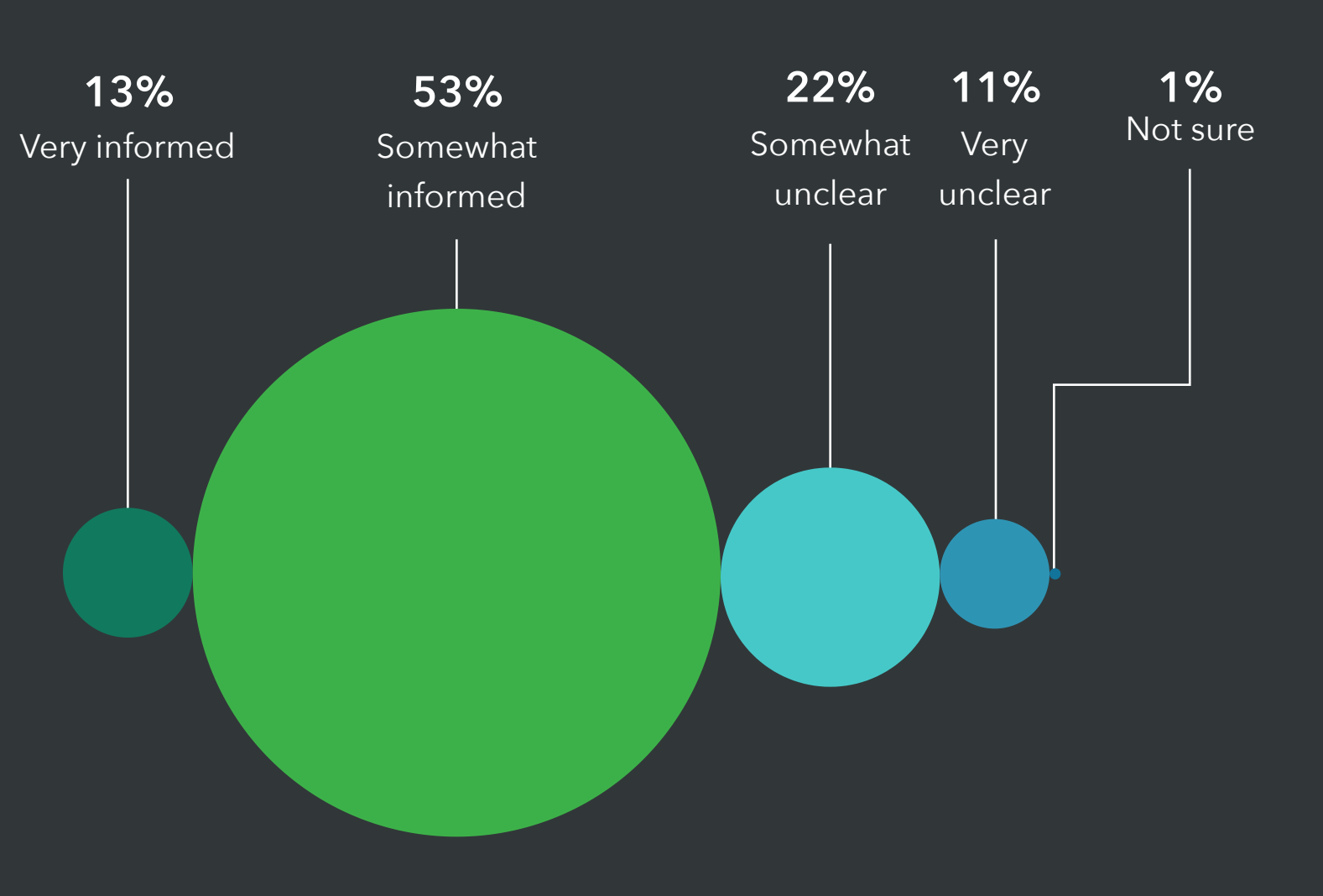
Data collection: Aug 17 - Nov 14, 2021

Respondents: 175 tech decision-makers in the US

Decision-makers are somewhat informed about the US Government's recent cybersecurity announcements

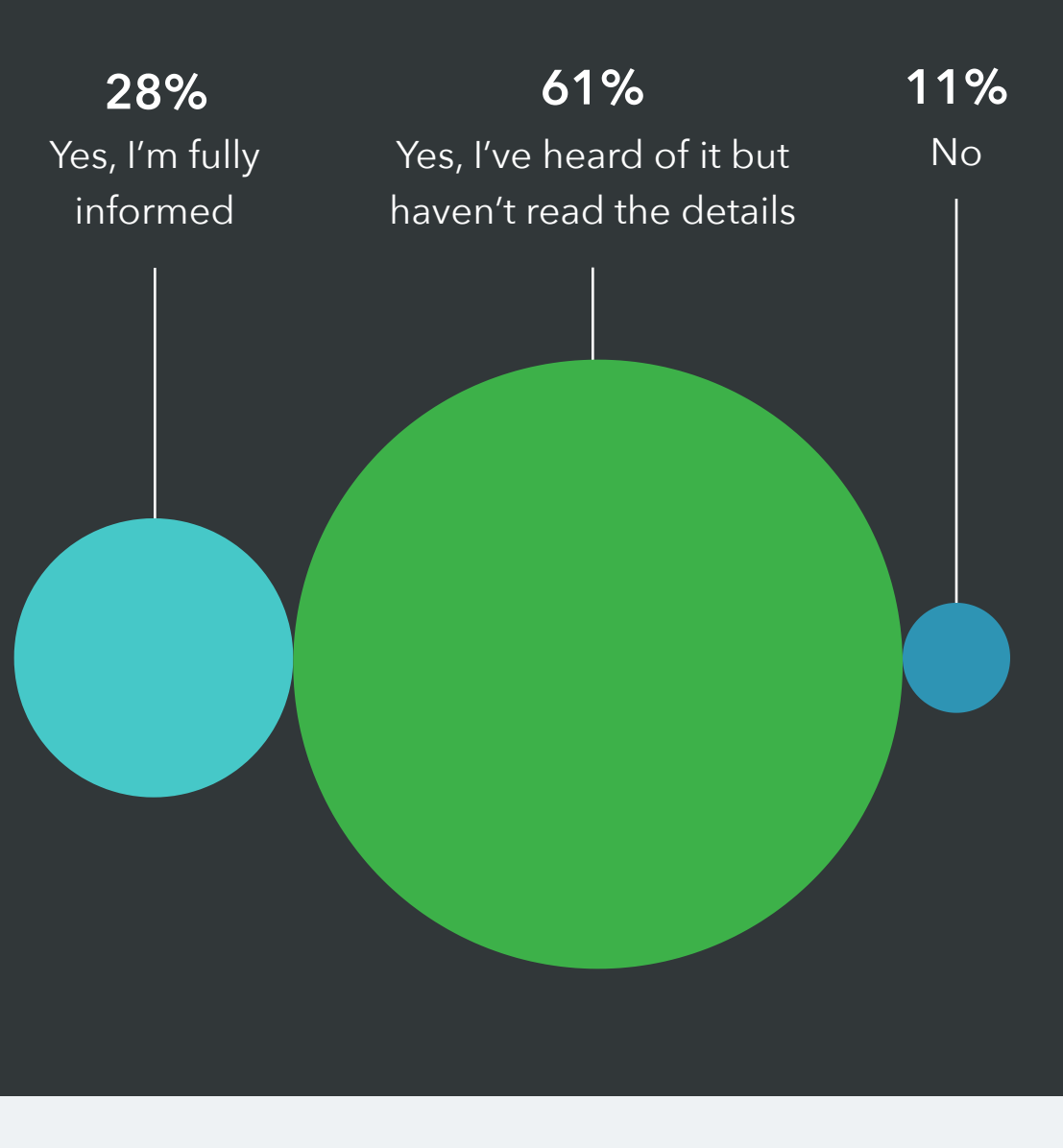
63% of decision-makers feel at least somewhat informed about US Governmental Task Forces. However, a third (33%) feel at least somewhat unclear.

How informed do you feel about the various US Governmental cybersecurity Task Forces?
(e.g., NCSL Cybersecurity Task Force, Justice Department's Cyber-Digital Task Force, CISA Cybersecurity Services, IST Ransomware Task Force)



As for President Biden's Executive Order on Improving the Nation's Cybersecurity, only just over a quarter (28%) feel fully informed, with most (61%) having heard of it without reading the details.

Are you aware of President Biden's Executive Order on Improving the Nation's Cybersecurity?



"I believe that the intent is solid and the result, if executed well, will improve our security posture."

C-suite, large software company

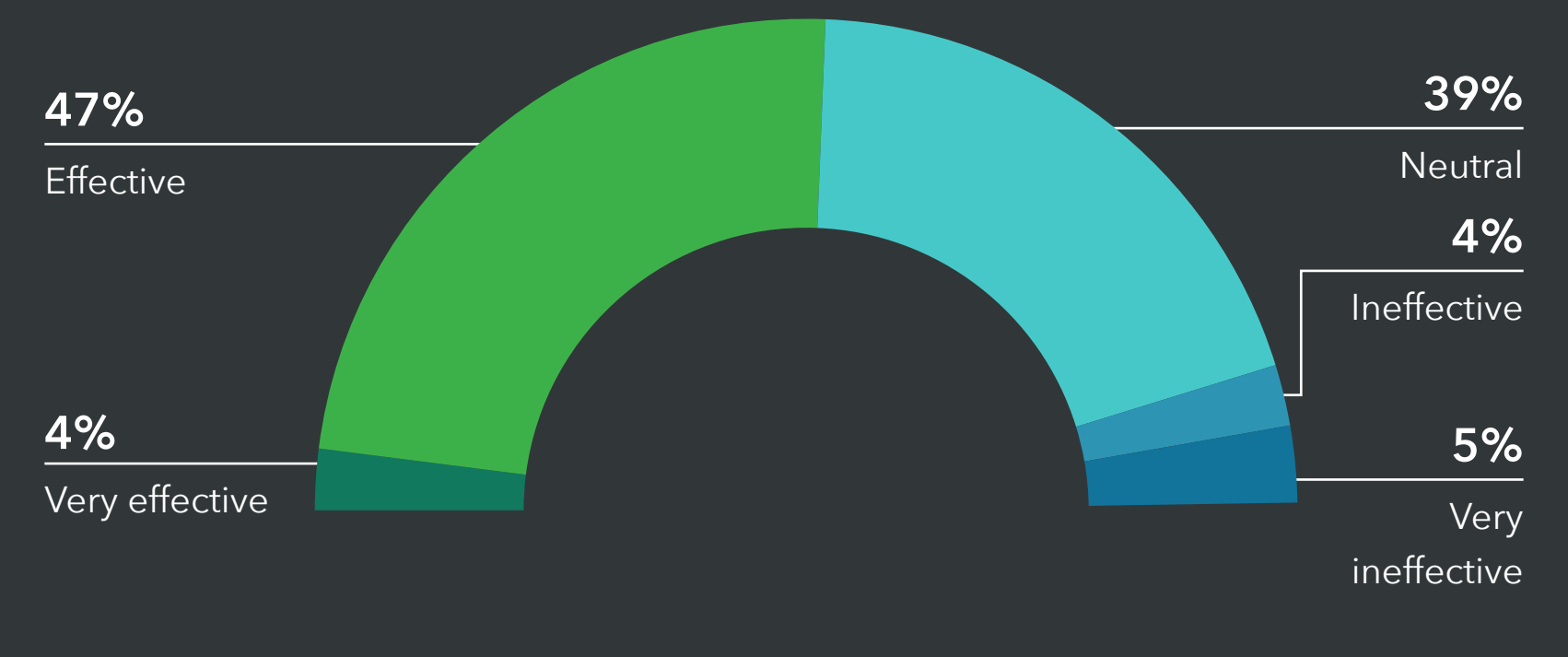
"It needs to be done with input from the private sector."

VP, large software company

Decision-makers are split over whether US Government cybersecurity initiatives will be effective

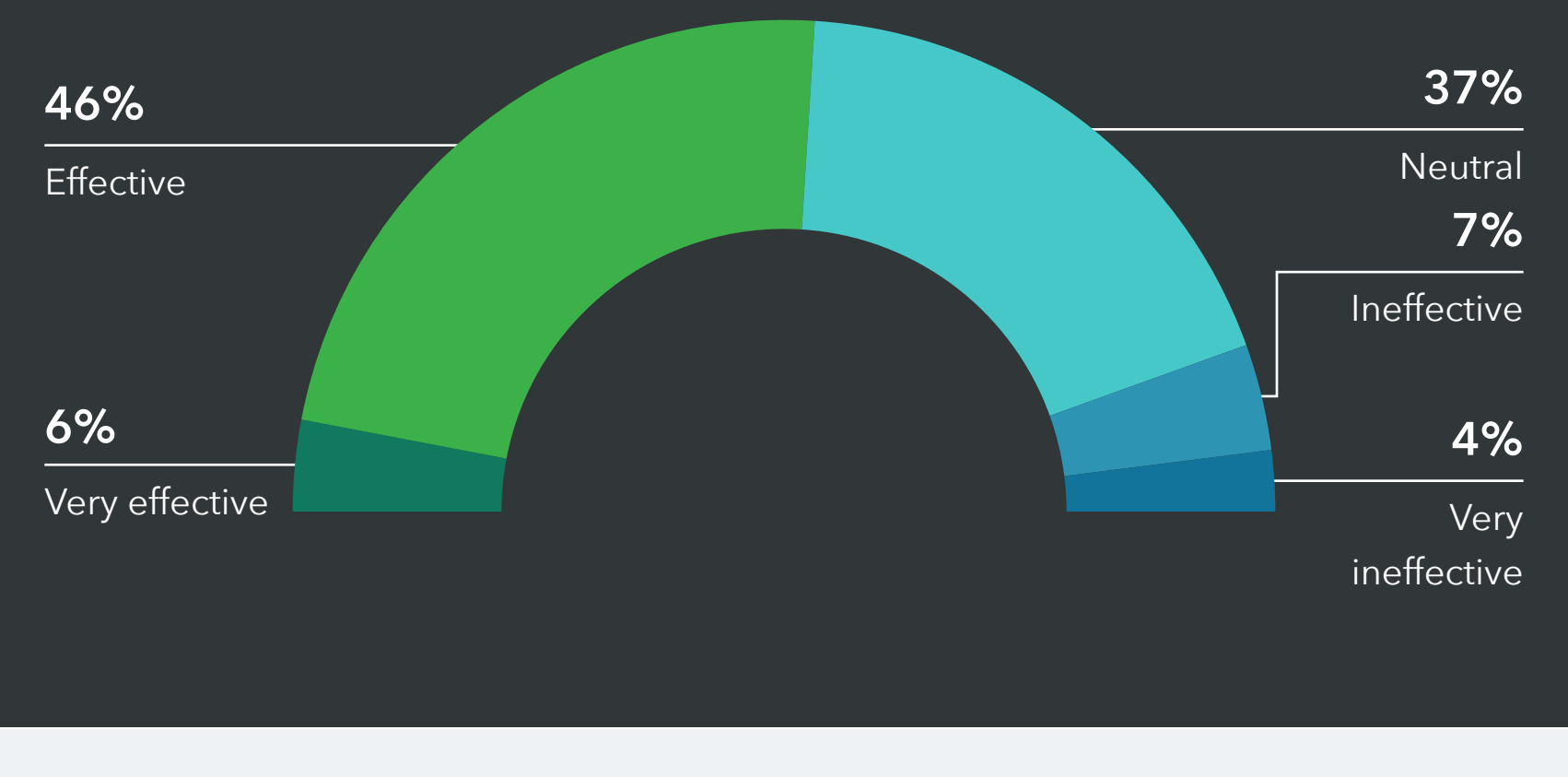
Just over half (51%) of decision-makers believe that Governmental cybersecurity Task Forces will be effective at improving business security in the US.

Do you believe Governmental cybersecurity Task Forces will be effective at improving business security in general in the US?



As for governmental digital infrastructure, similarly, just over half (52%) believe that Governmental cybersecurity Task Forces will provide effective protection.

Do you believe Governmental cybersecurity Task Forces will be effective at protecting governmental digital infrastructure in the US?



"It's not going to work. Tech leaders at organizations of every size need to COLLABORATE to come up with a real solution."

Director, medium-sized education company

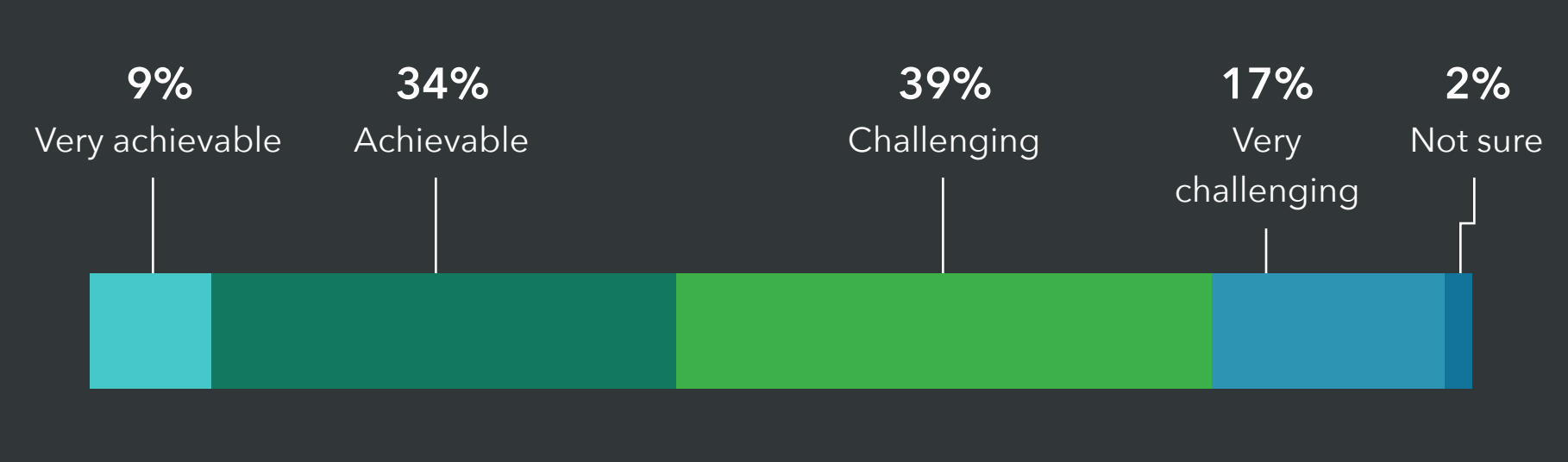
"Anybody who has ever worked for a state, federal, or local government understands that the public sector is so ridiculously behind the times and tied up with administrative overhead and bureaucracy that they will never be the leading edge of cybersecurity."

Director, large finance company

Most consider the timelines laid out for US Governments agencies challenging, but would begin by prioritizing Zero Trust implementation

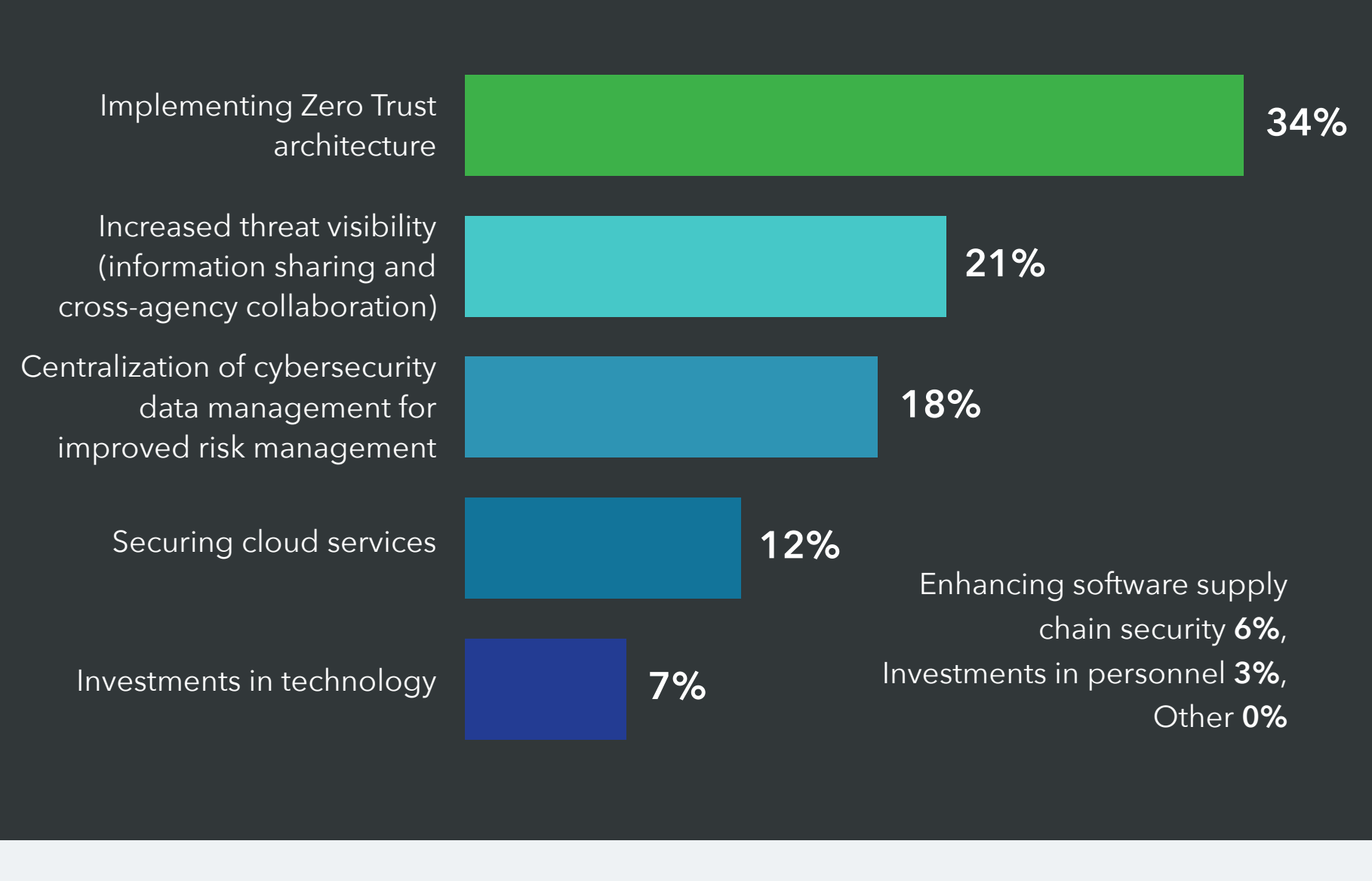
Regarding the recent Executive Order that gave Government agencies 180 days to implement multi-factor authentication and data encryption protocols, more decision-makers (56%) consider that timeline challenging than achievable (43%).

Government agencies were recently given 180 days to implement multi-factor authentication and encryption for data at rest and in transit. Based on your experiences, do you think this timeframe is achievable?



As for the Executive Order that detailed several priorities for Government agencies to immediately improve upon, most (34%) decision-makers would begin by implementing Zero Trust architecture, while 21% would start with increasing threat visibility.

President Biden's Executive Order on Improving the Nation's Cybersecurity laid out priority areas for Government agencies to immediately improve on. Which of the following would you prioritize first:



"As with any organization, the strategy planning is going to be an important part of this. Without an effective strategy, the rest falls apart. Not sure if the feds have the strategic capability to pull this off."

Director, large software company

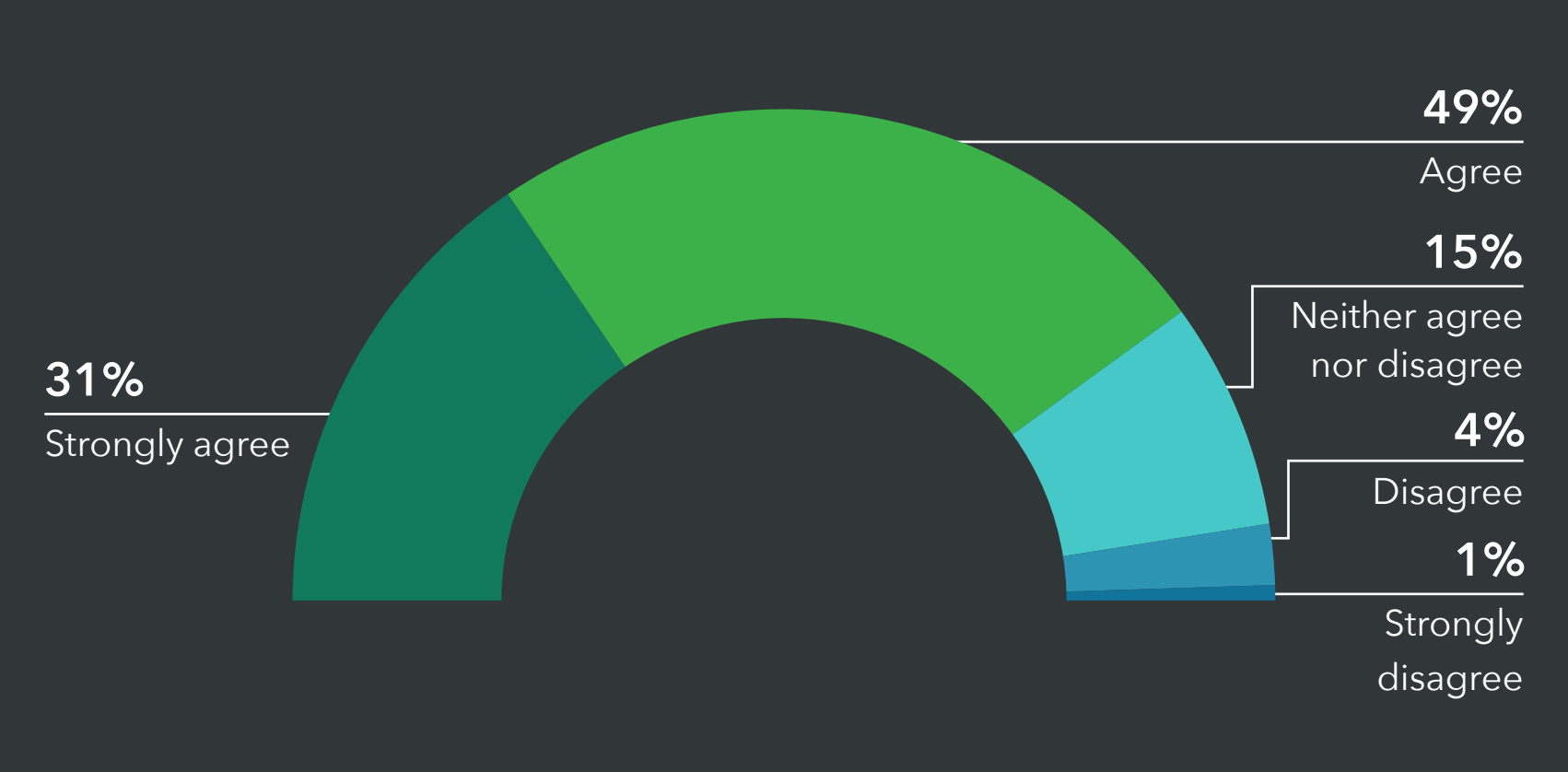
"I like the initiative but it's very complex."

C-suite, medium-sized software company

While most agree that the US needs standardized cybersecurity regulations, there is concern that legacy technologies and skills gaps might hold efforts back– and right now, the bad actors are in a stronger position

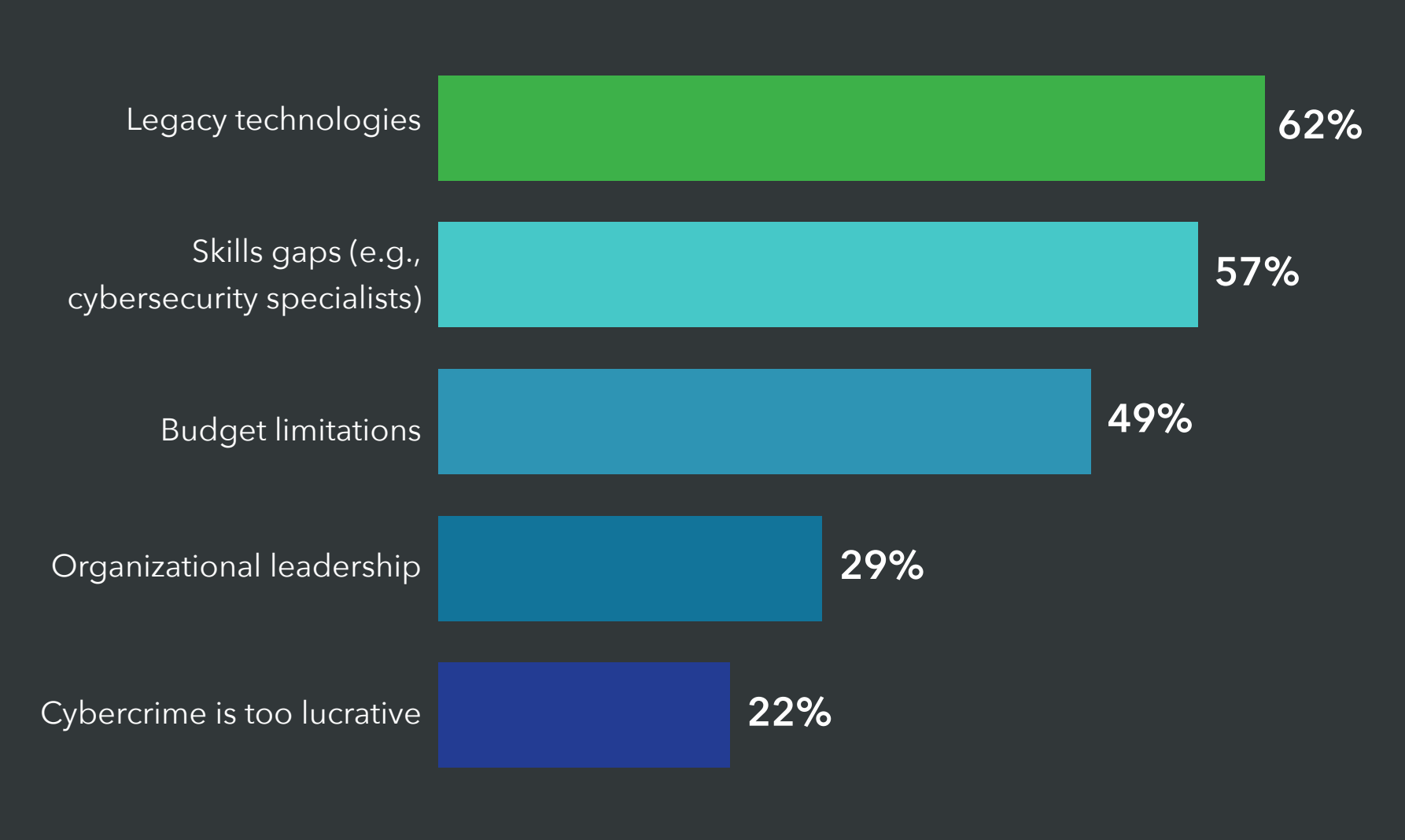
80% of decision-makers agree that the US needs standardized cybersecurity regulations.

To what extent do you agree with the following: "The US needs standardized cybersecurity regulations."



When it comes to developing a coordinated nation-wide approach to cybersecurity in the US, the top challenges noted are legacy technologies (62%), skills gaps (57%), and budget limitations (29%).

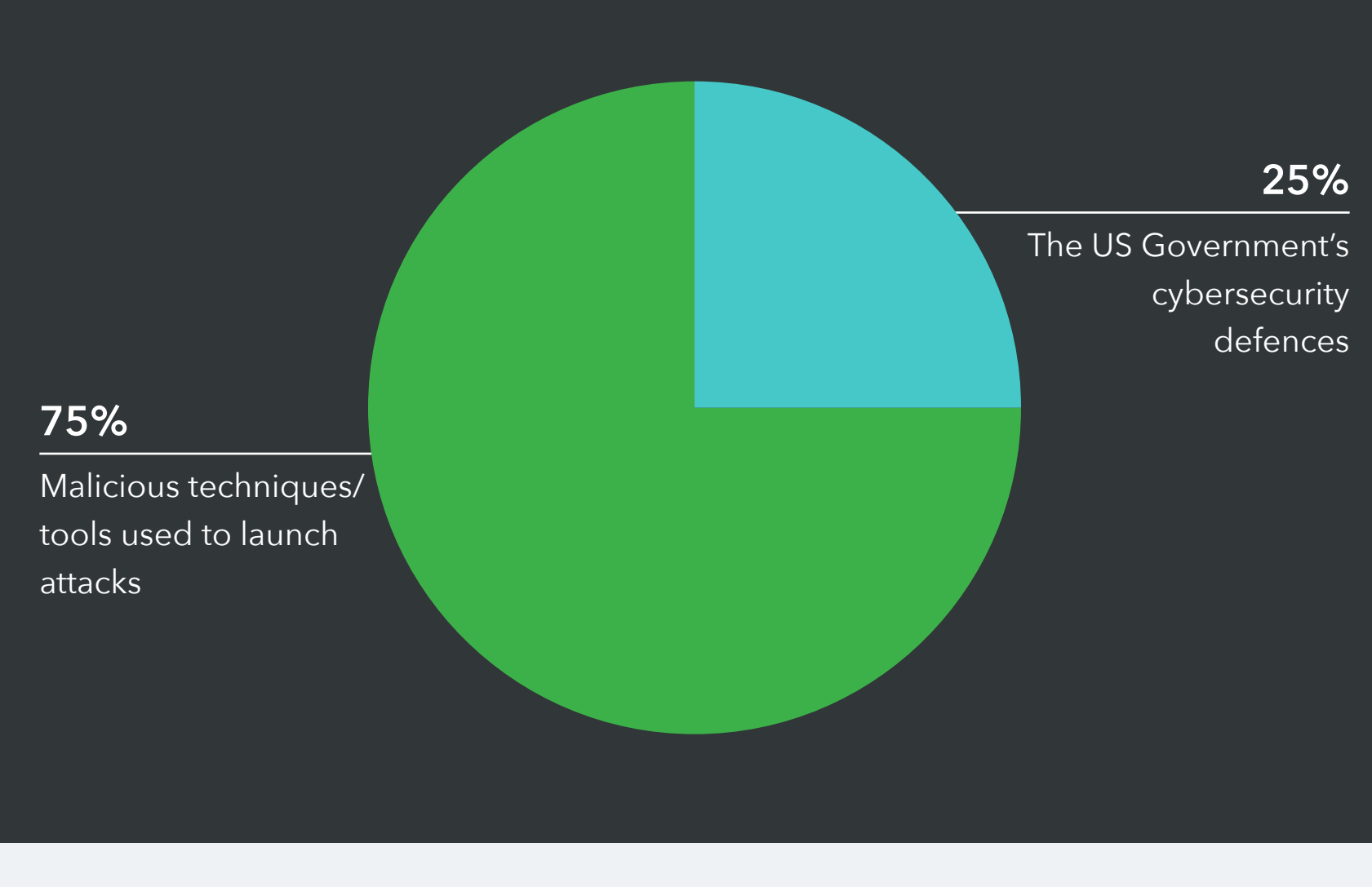
Which of the following do you view as the top 3 challenges to a coordinated nation-wide approach to cybersecurity in the US?



Inability to effectively audit organizational compliance **22%**, Insufficient punishments for organizations that don't comply **21%**, Strategy isn't robust/thorough enough **21%**, Non-technical executive buy-in **20%**, Board buy-in **14%**, Employee buy-in **14%**, None of these **1%**, Other **1%**

Three times as many respondents (75%) believe that currently, the malicious techniques/tools used to launch attacks are in a stronger position than the US Government's cybersecurity defences.

Which do you think is in a stronger position currently: The US Government's cybersecurity defences or malicious techniques/tools used to launch attacks?



"Security education plays a key unappreciated role."

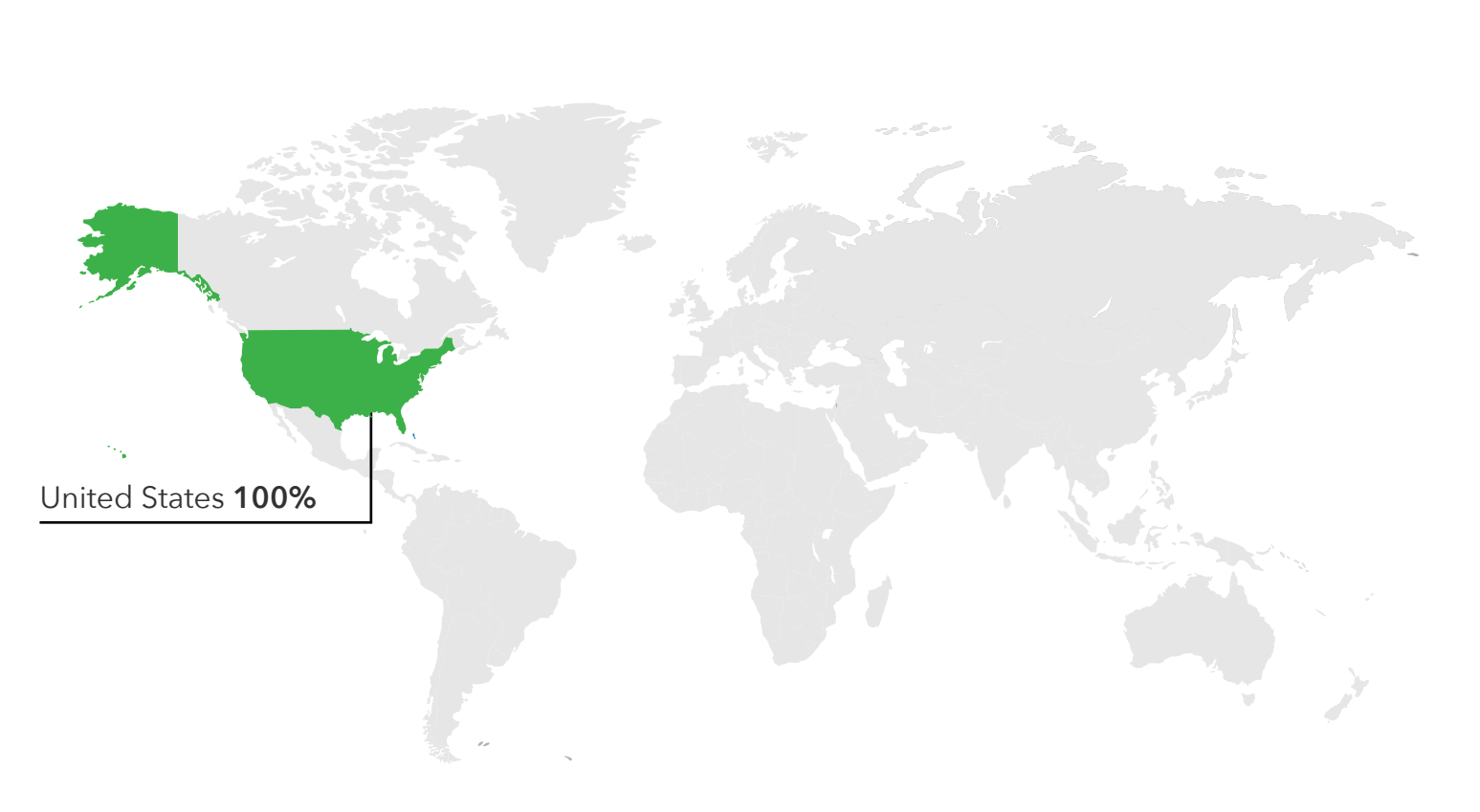
Director, large software company

"Government efforts will likely produce limited success, at best. Would probably need to focus on broad standards and frameworks, something NIST does well, and let industry innovate and figure out the details. Unfortunately, the threats are very asymmetrical - bad actors only need to succeed once, the defenders need to be successful 100% of the time."

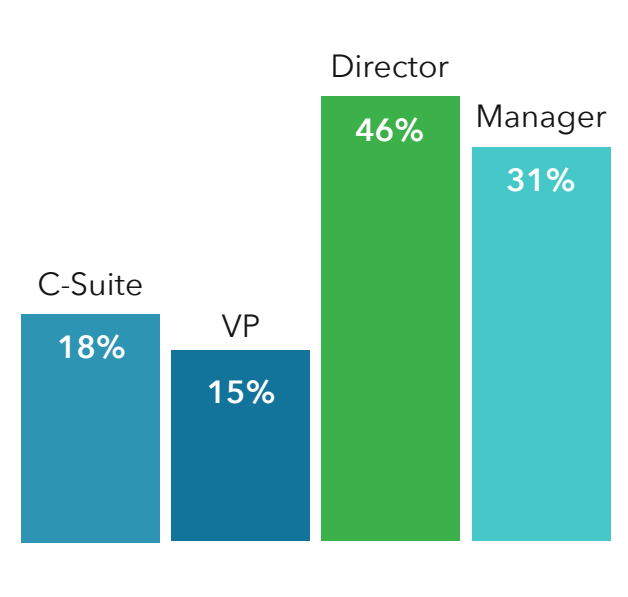
C-suite, medium-sized software company

Respondent Breakdown

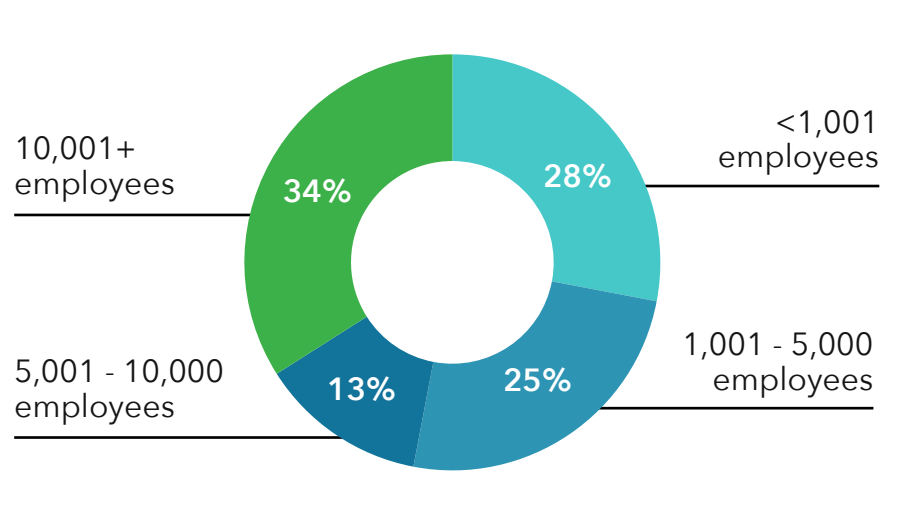
Region



Title



Company Size



References:

[1] Executive Order on Improving the Nation's Cybersecurity, May 12, 2021 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Insights powered by PULSE