PULSE
kiuwan
An Idera, Inc. Company

Securing the Software Supply Chain

Modern organizations are run on software from myriad sources, including third-party apps whose own software may have come from a variety of open source projects, creating complex software supply chains. Following high-profile software supply chain attacks, such as SolarWinds in 2020, how do decision-makers approach software supply chain risk in their organization?

In this One-Minute Insight Report, Pulse surveyed almost 300 tech leaders to understand:

- If software supply chain security is a priority within their organization
- Whether they've been impacted by breaches and how vulnerable they feel
- What tools are being used and the main reasons attacks happen

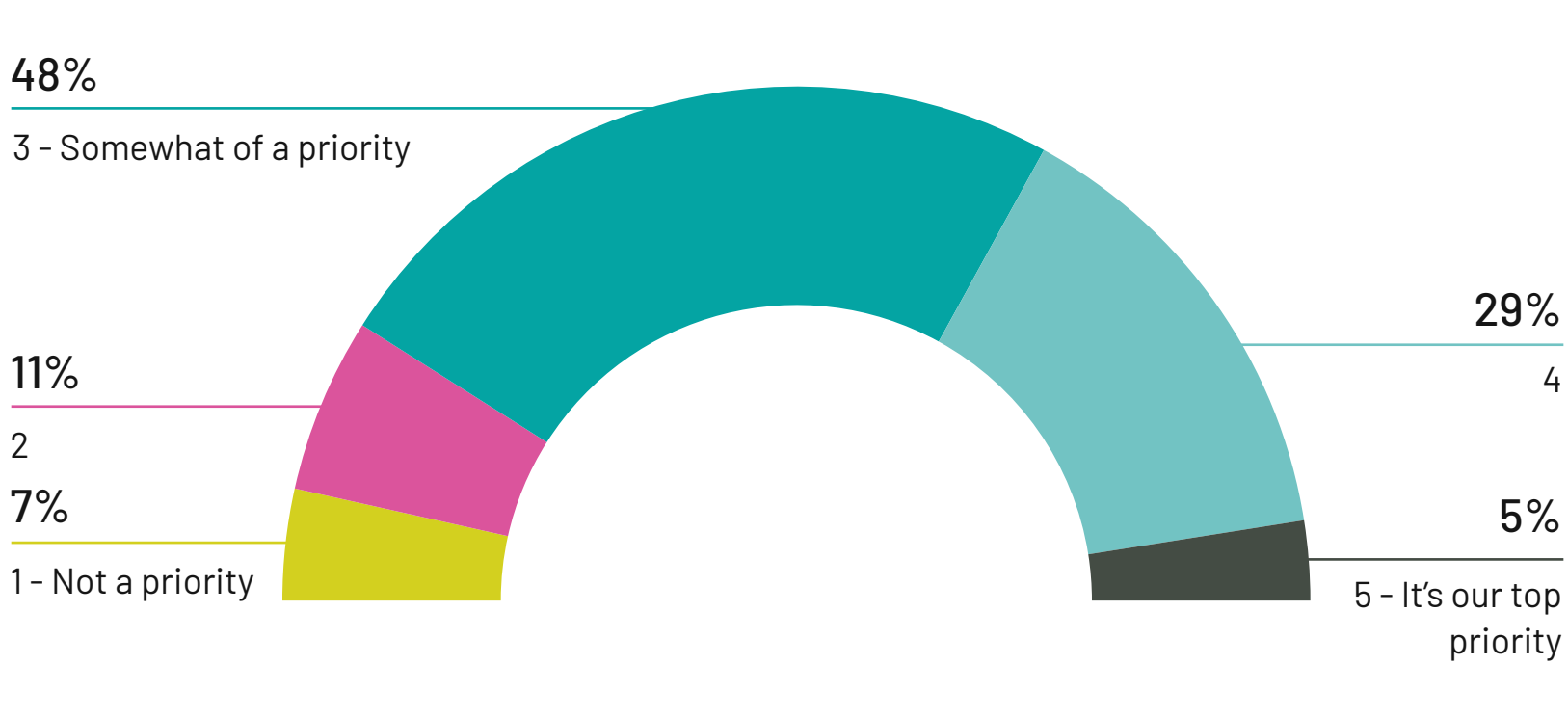
Data collected from May 21 - Aug 2, 2021

Total respondents: 298 tech leaders

Software supply chain security is a priority for most leaders—though many don't address it in their cybersecurity strategy

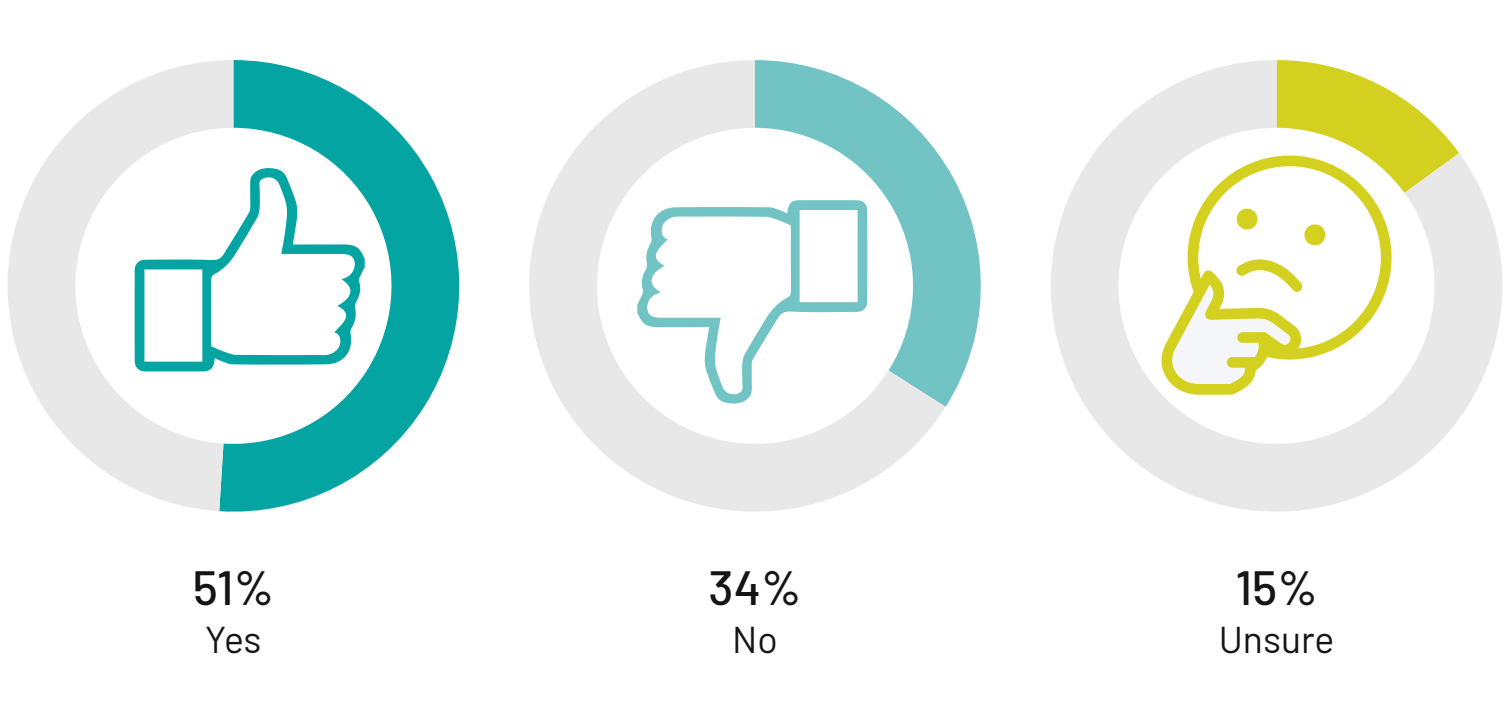
82% of decision-makers view software supply chain security as at least somewhat of a priority. Only 7% outright report that it isn't a priority in their organization.

On a scale of 1-5, how high of a priority is software supply chain security at your organization?



However, only just over half (51%) report that the software supply chain is addressed in their organizational cybersecurity strategy.

Is the software supply chain specifically addressed in your organization's cybersecurity strategy?



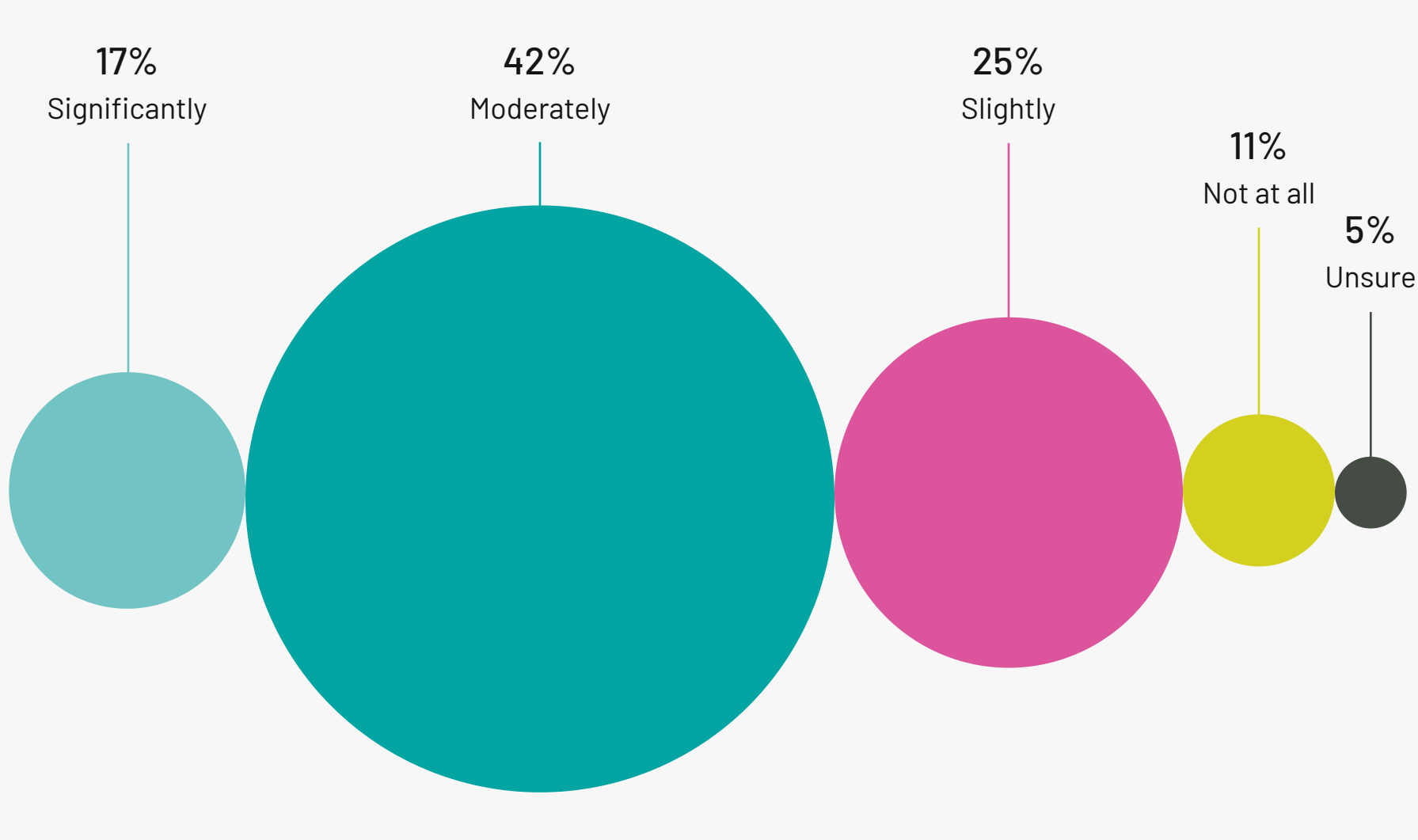
"[Software supply chain security,] if not attended to right now, will be a major issue in the future."

- C-suite, finance company

Many have increased software supply chain security prioritization this year—even though most remain unaffected directly

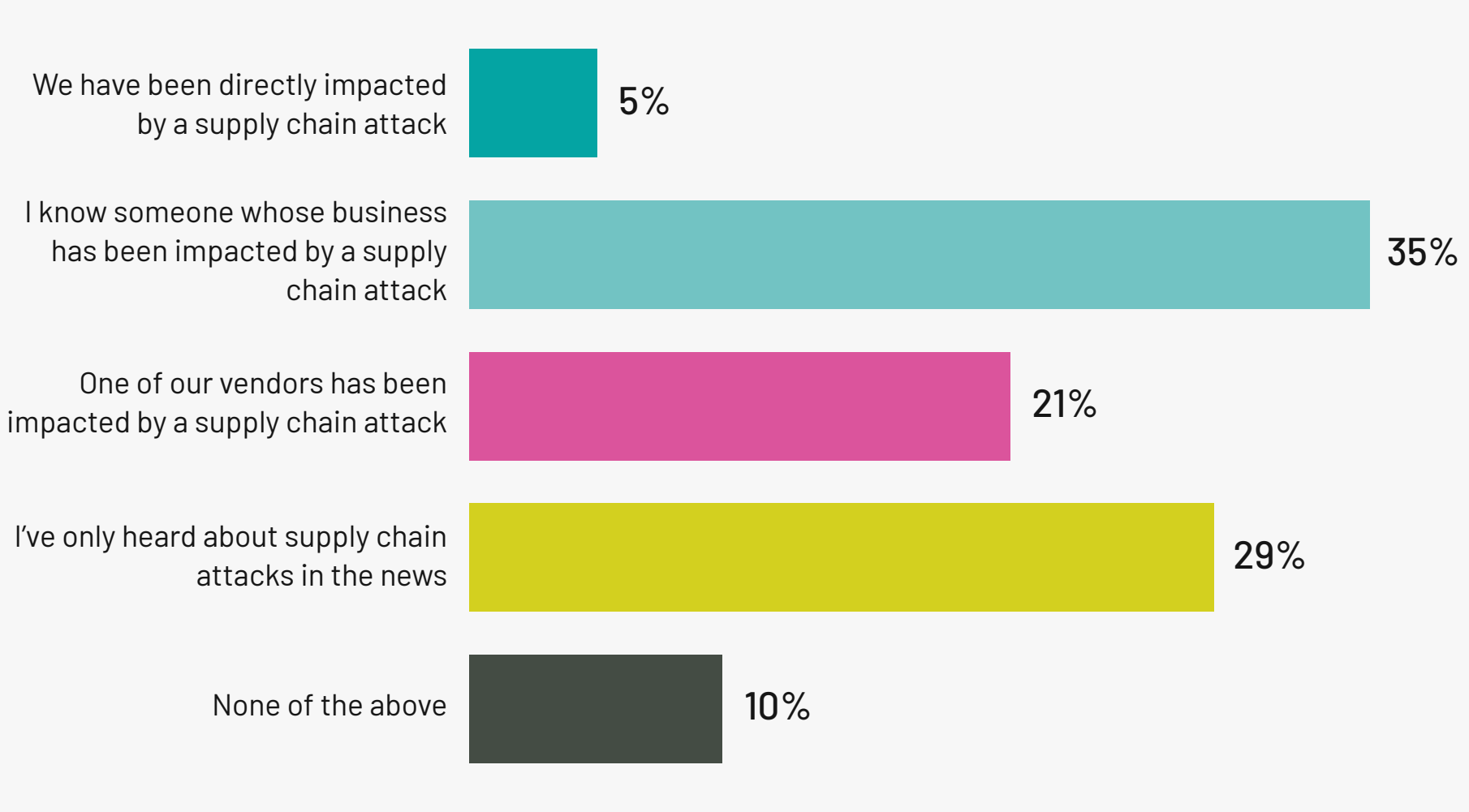
84% overall report that supply chain security has become more of a priority over the past year.

Has supply chain security increased in priority within your organization over the last year?



That increased priority comes despite the fact only 5% report that their organization has been directly affected by recent, high-profile software supply chain attacks. However, over a third (35%) know someone whose business has been impacted.

How would you describe the impact on your organization of recent, well publicized software supply chain attacks?



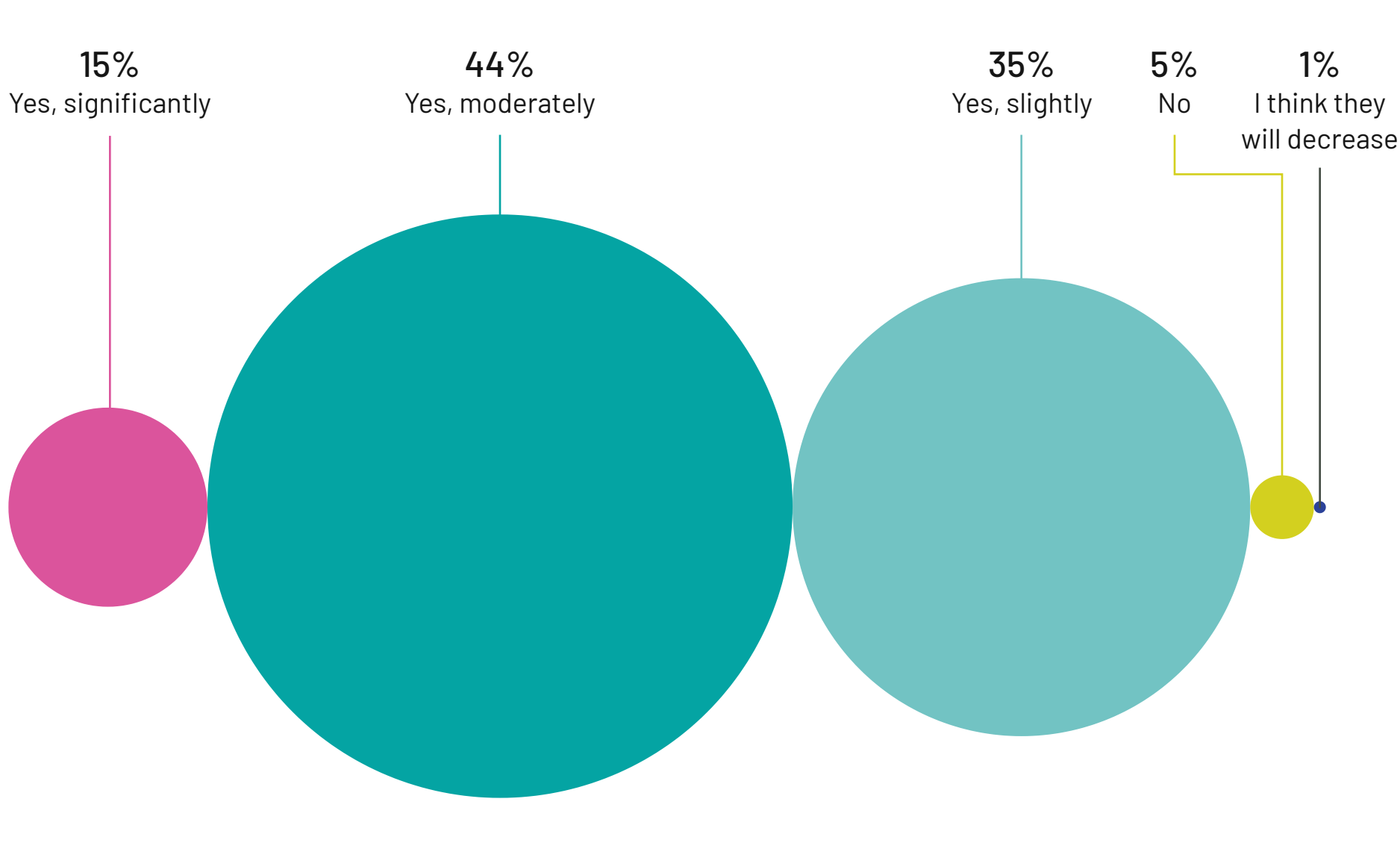
"This has been a recent topic of conversation and we are changing our internal processes/tools to reflect this disturbing upward trend."

- C-suite, software company

Tech leaders anticipate supply chain attacks to increase, but not necessarily on their business

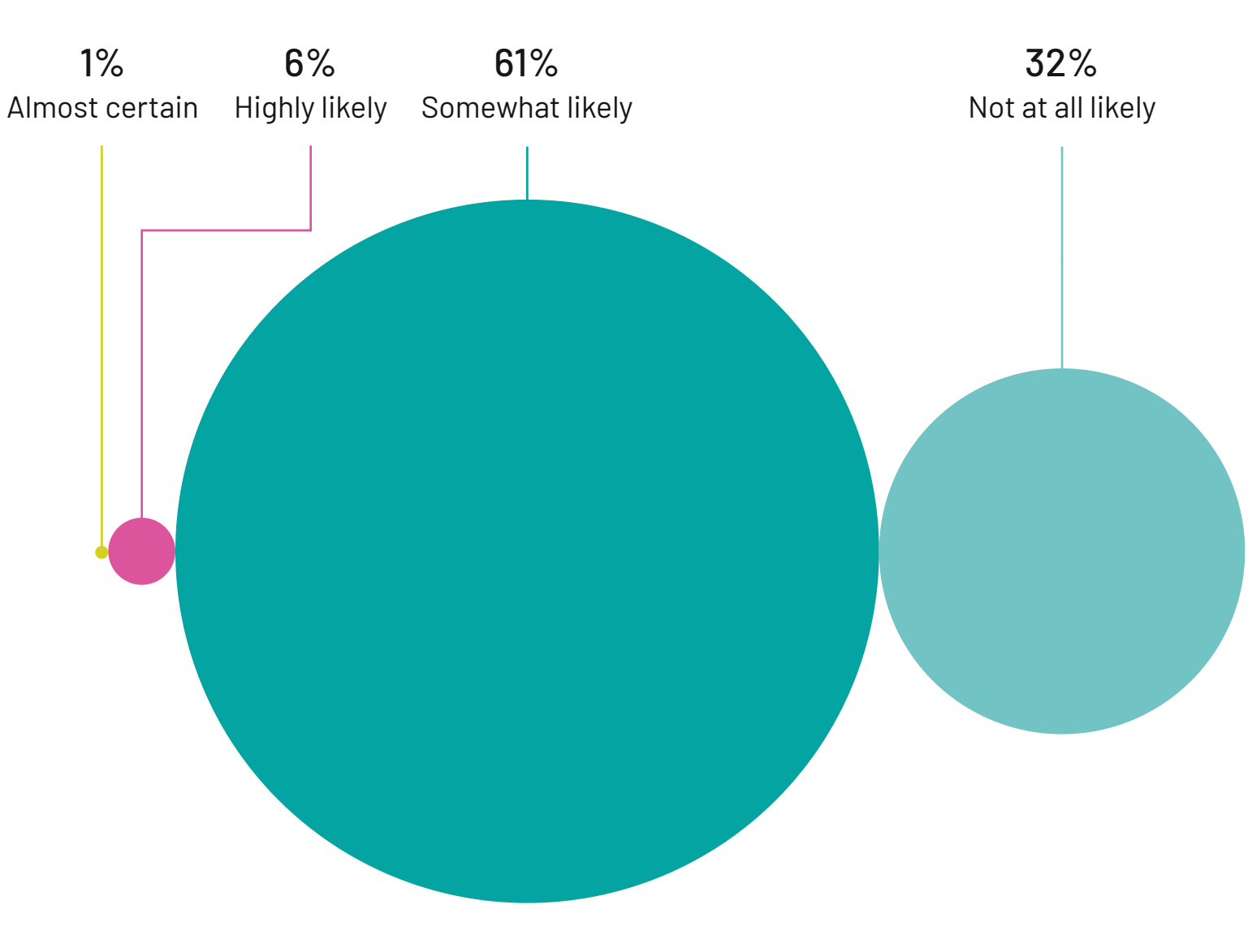
94% of tech leaders believe software supply chain attacks will increase over the next 12 months, with most (44%) expecting a moderate increase.

Do you believe supply chain attacks will increase over the next 12 months?



However, while over half (61%) believe an attack on their organization's software supply is somewhat likely over the next 12 months, almost a third (32%) think that scenario is not at all likely.

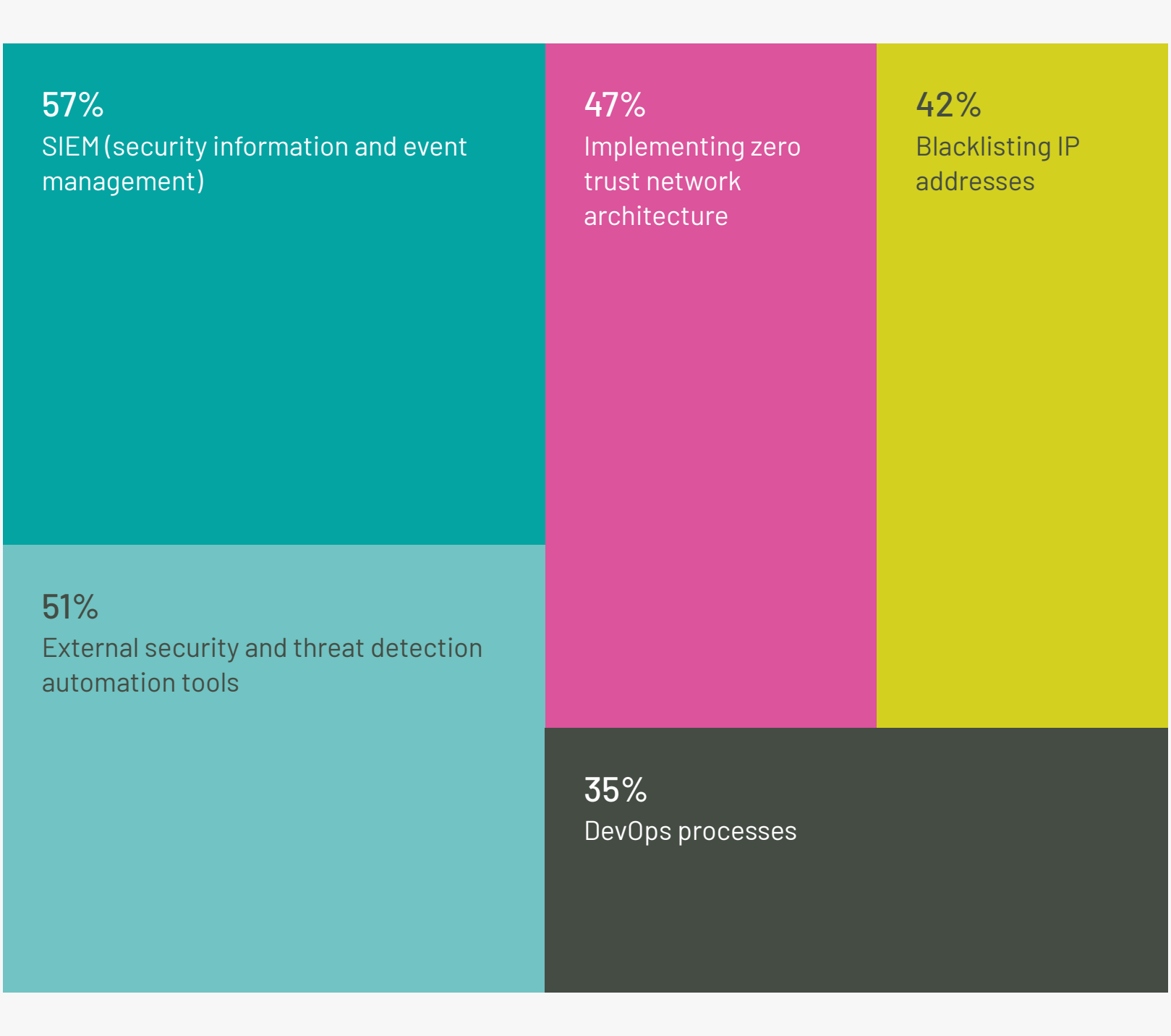
How likely do you think it is that your company will be a victim of a supply chain attack in the next 12 months?



SIEM is the main tool leaders are using to mitigate risk, with employees highlighted as the main vulnerability point for software supply chain incidents

To protect against software supply chain attacks, most already have security information and event management (SIEM) tools (57%) and external security and threat detection tools (51%).

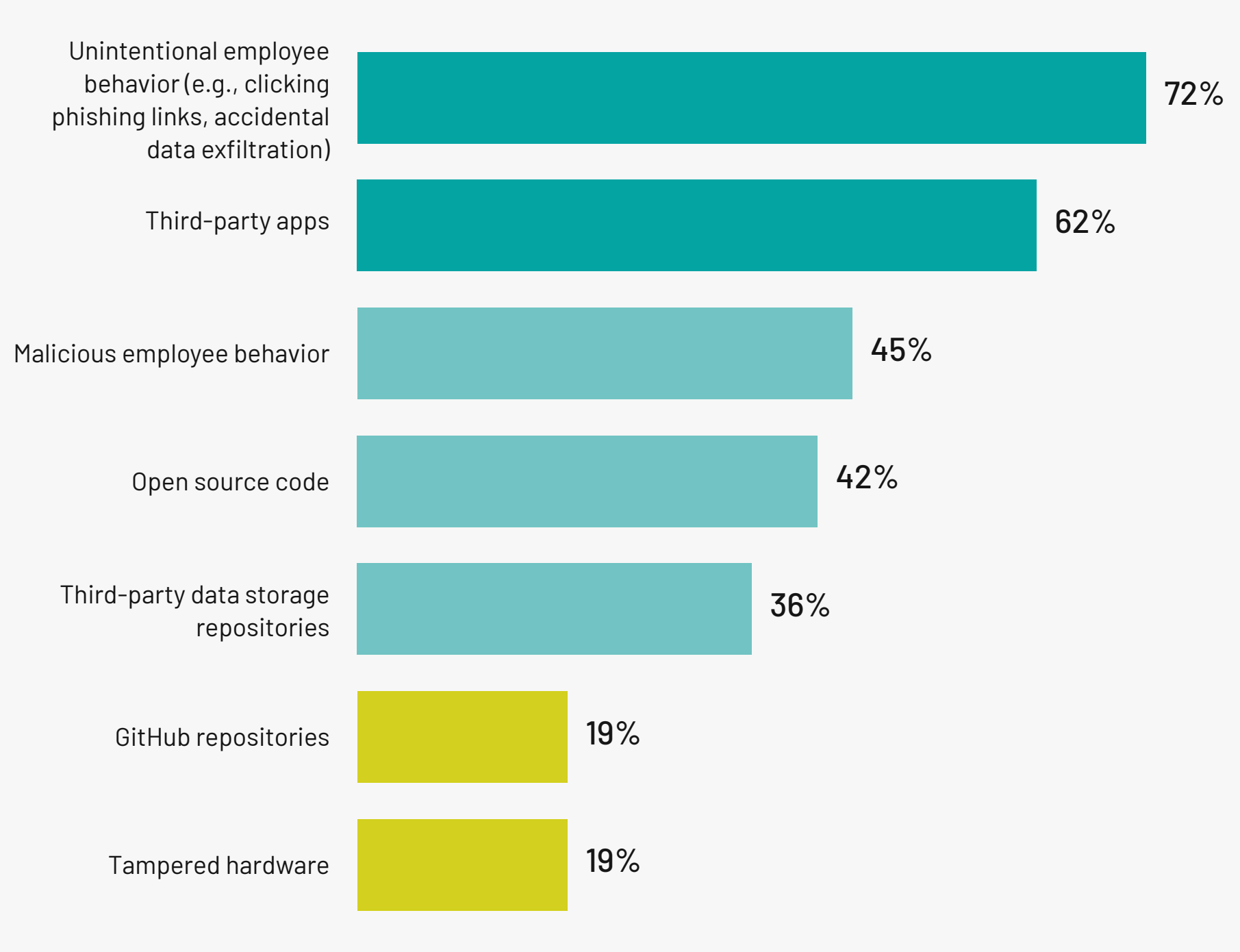
What measures are you currently taking to mitigate software supply chain risk?



Requiring vendors to produce minimum compliance certification standards (e.g., SOC 2) **34%**, Software supply chain audits **28%**, Partnering with an MSSP (Managed Security Services Provider) **23%**, Requiring source code access from all third party software providers **15%**, Requiring an S BOM (Software Bill of Materials) for vendors **10%**, None of these **5%**

Unintentional behavior from employees (such as clicking on phishing links) is viewed as the most vulnerable entry-point for software supply chain attacks (72%), with third-party apps (62%) also considered a top vulnerability by most.

What do you see as the key entry-point vulnerabilities for supply chain attacks?



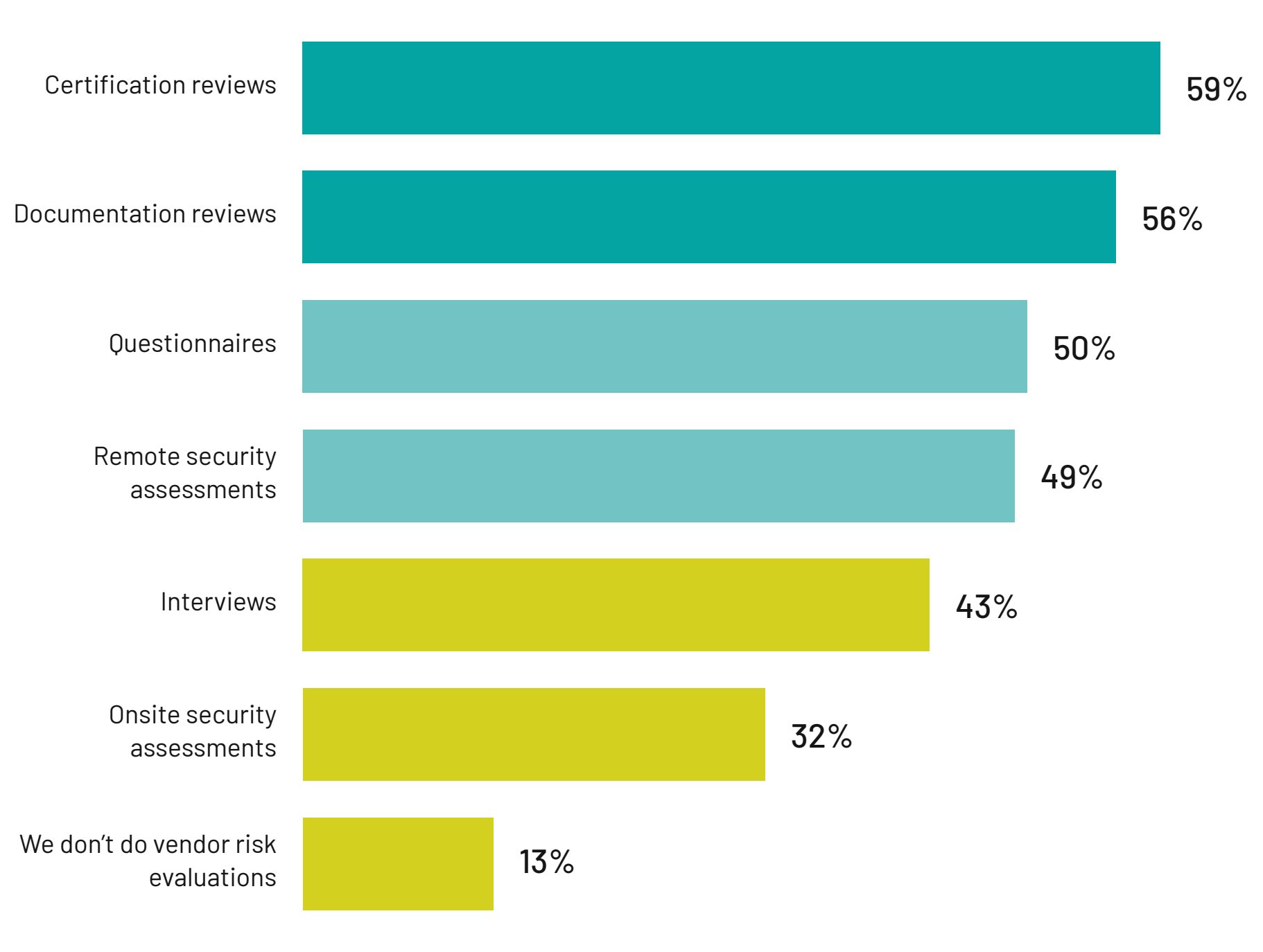
"[Software supply chain security is a] huge focus for us. All app dev teams are going through secOps training with champions embedded in every org."

- C-suite, software enterprise

Third-parties are vetted primarily through certification reviews—though many don't trust vendors to immediately disclose supply chain breaches

Leaders evaluate third-party software supply chain risk primarily through certification reviews (59%), documentation reviews (56%), and questionnaires (50%).

How do you currently evaluate vendor risk to your software supply chain?



Over half (59%) agree that vendors can be trusted to immediately disclose supply chain breaches—leaving 41% of decision-makers who don't find vendors trustworthy in this matter.

To what extent do you agree with the following: "Third party vendors can be trusted to disclose supply chain breaches as soon as they become known?"

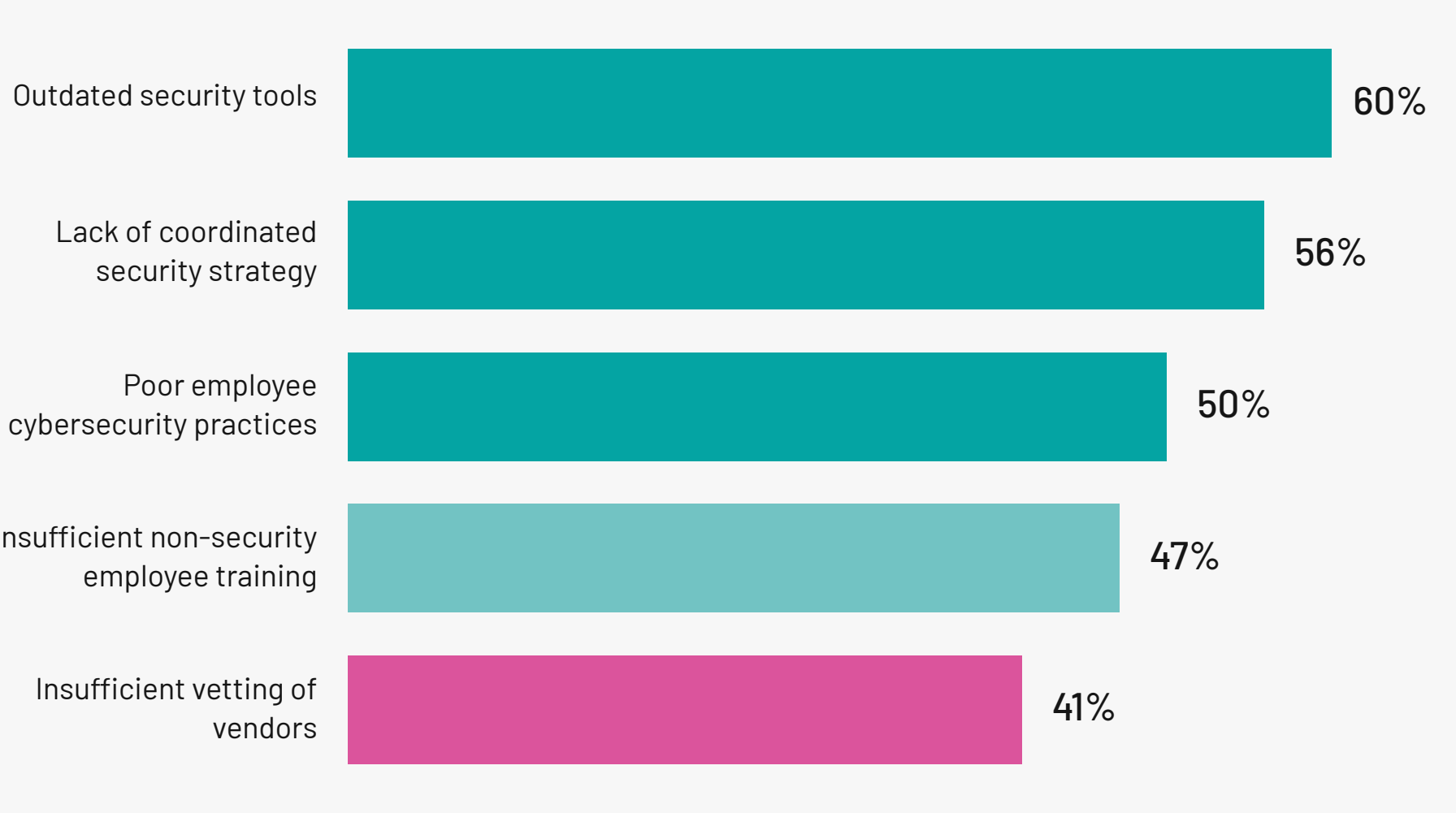
"[A] complete review and auditing process is critical to secure [the] software supply chain."

- VP, transportation company

Old security tools to blame for software supply chain attacks—and risk management should fall on the CISO's shoulders

Leaders believe software supply chain attacks are made possible primarily through outdated security tools (60%), lack of coordinated security strategy (56%), and poor employee cybersecurity practices (50%).

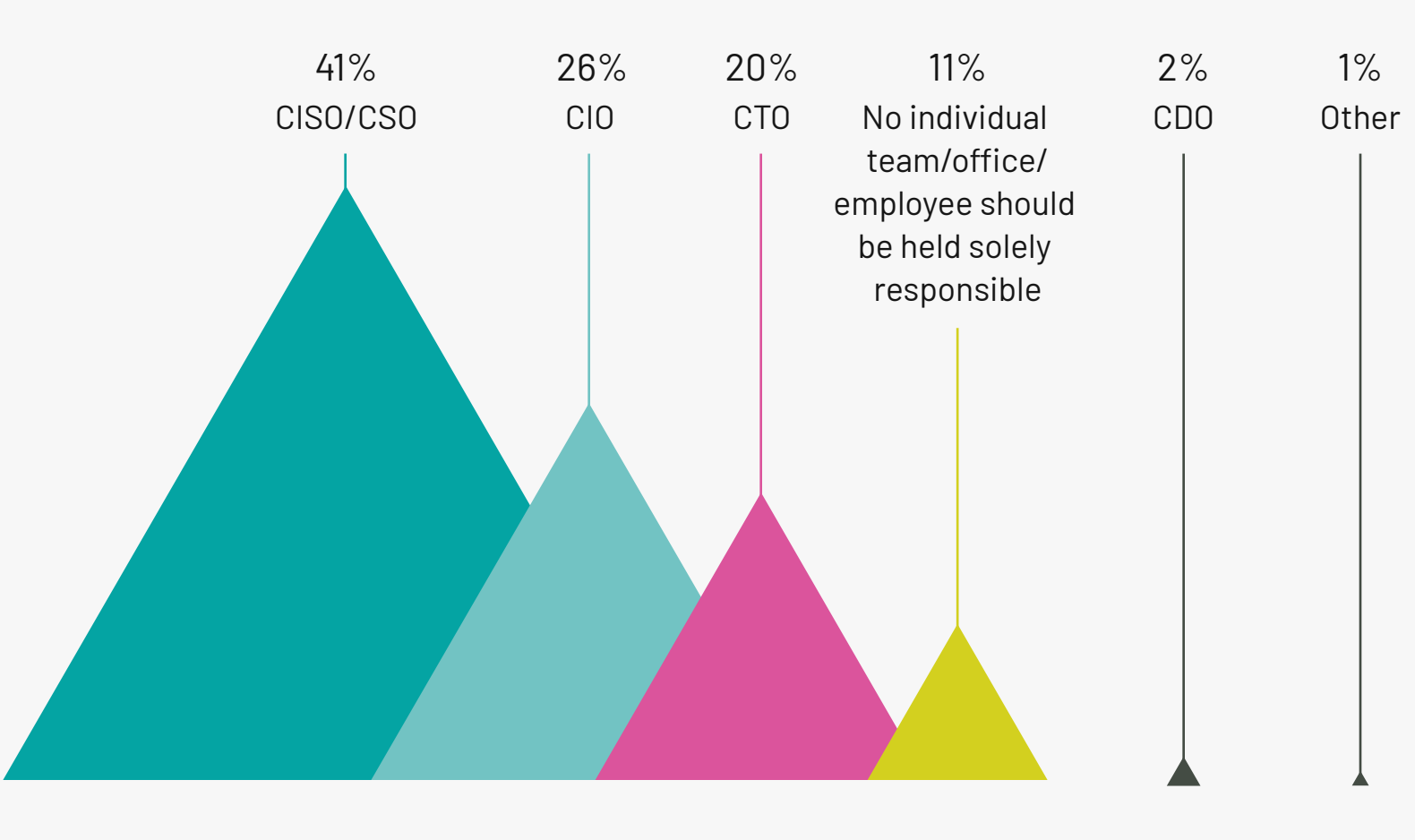
Looking from within an organization, what are the main reasons a company falls victim to a software supply chain attack?



Insufficient security budget **33%**, Overreliance on manual protocols over automated protocols **31%**, Overreliance on third party security tools **28%**, Unwillingness from business executives to take cybersecurity risks seriously **28%**, Lack of security talent **27%**, Overreliance on on-prem security tools **26%**, None of these **2%**

Most (41%) believe it is the CISO/CSO's responsibility to evaluate software supply chain risk.

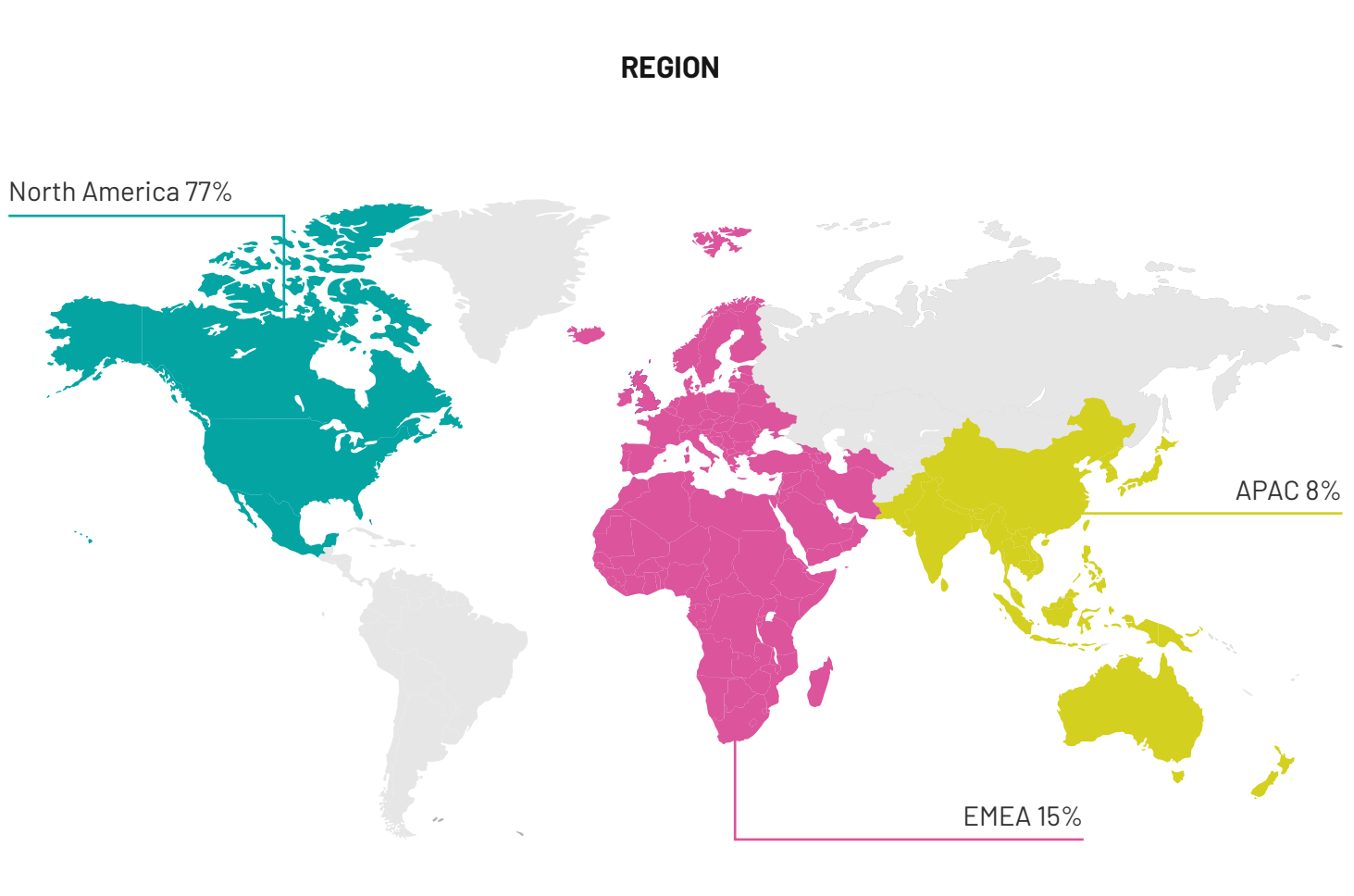
Which team / whose office is responsible for evaluating software supply chain risk?

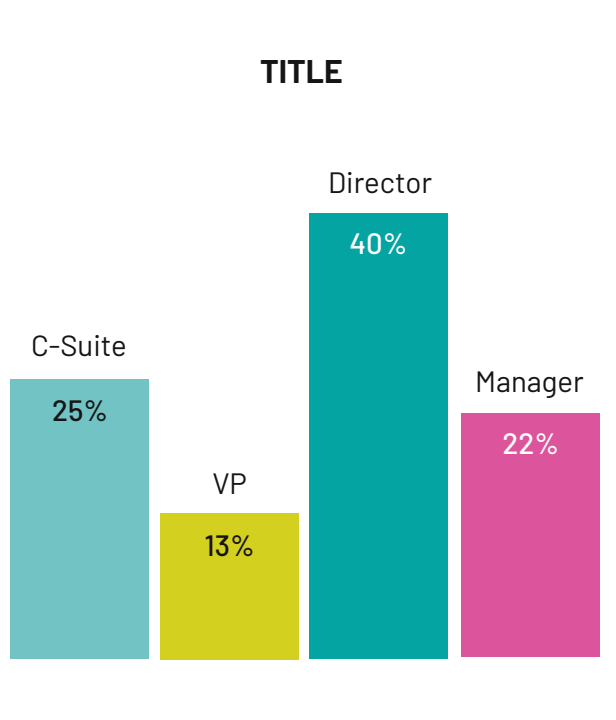


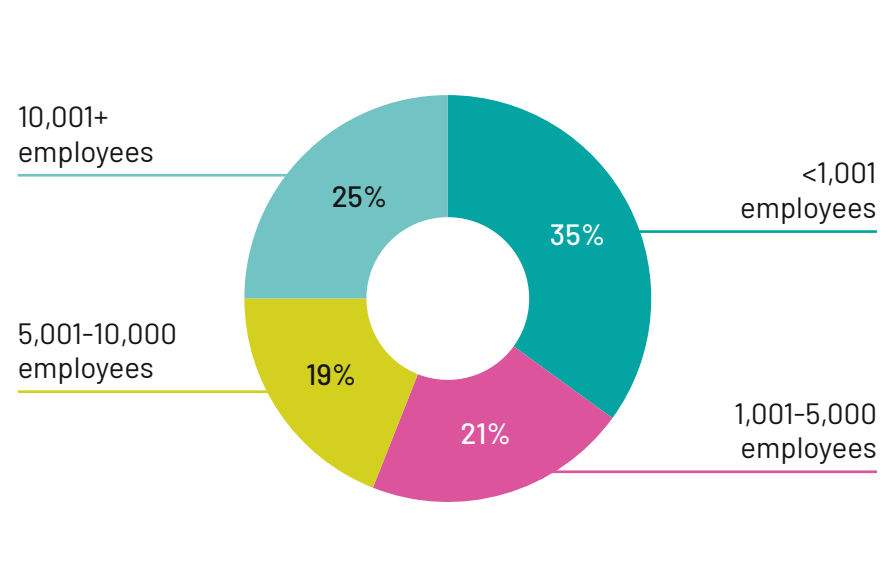
"Vendor regulations [for software supply chains] are coming."

- C-suite, software enterprise

Respondent Breakdown







Insights powered by PULSE