Cybersecurity: how do you rise above the waves of a perfect storm?

EY Global Information Security Survey 2021

The better the question. The better the answer.
The better the world works.

EY
Building a better
working world

“

Speed of change comes with a heavy price. The need for rapid transformation meant that businesses often overlooked security. The risk of moving on without addressing these gaps, as businesses maintain new working practices in the post-COVID-19 era, is increasingly urgent. Recent ransomware events underscore how critical immediate action is.

Kris Lovejoy

Global Cybersecurity Leader

EY

About the survey

The EY Global Information Security Survey 2021 draws on insights from over 1,400 chief information security officers (CISOs) and senior security executives. It explores the challenges they face as they position their function as an enabler of growth and strategic partner.

1,430 senior executives	Global reach	Large companies	Cross-sector sample
25% CISO	**51 countries worldwide:**	**Annual revenues:**	**6 core sectors:**
29% Other C-suite roles	**45%** EMEIA	**23% Over** $10b	▸ Financial services ▸ Consumer products and retail ▸ Health and life sciences ▸ Energy ▸ Government and public sector ▸ Technology, Media & Entertainment, and Telecommunications
46% Senior security roles	**18%** APAC	**51%** $1-9.9b	
	36% Americas	**25%** $999m or less	

The survey was supplemented by in-depth interviews with leading security professionals, including:

- Roland Cloutier, Global Chief Security Officer, TikTok
- Darren Kane, Chief Security Officer, NBN Co
- Remo Marini, Chief Security Officer, Generali

Executive summary

The pandemic saw a significant rise in the number of cyber-attacks, many of which could have been avoided through security by design. But there is also opportunity ahead. CISOs today can position their role as enablers of growth – but first they need to resolve three core challenges:

1. The cybersecurity organization is severely underfunded – but funding is needed more than ever.

One in three respondents (36%) expects to suffer a major breach that could have been avoided through better investment.

2. Regulatory fragmentation is a headache, creating additional work and resourcing problems.

Half (49%) say compliance can be the most stressful part of their job, and more fragmentation is expected.

3. CISOs' relationships are weak – when strong connections are key to Security by Design

76% say colleagues do not bring them into initiatives until after the planning stage has finished.

Section 1

CISO at the crossroads

CISO at the crossroads
Key findings from our 2021 research

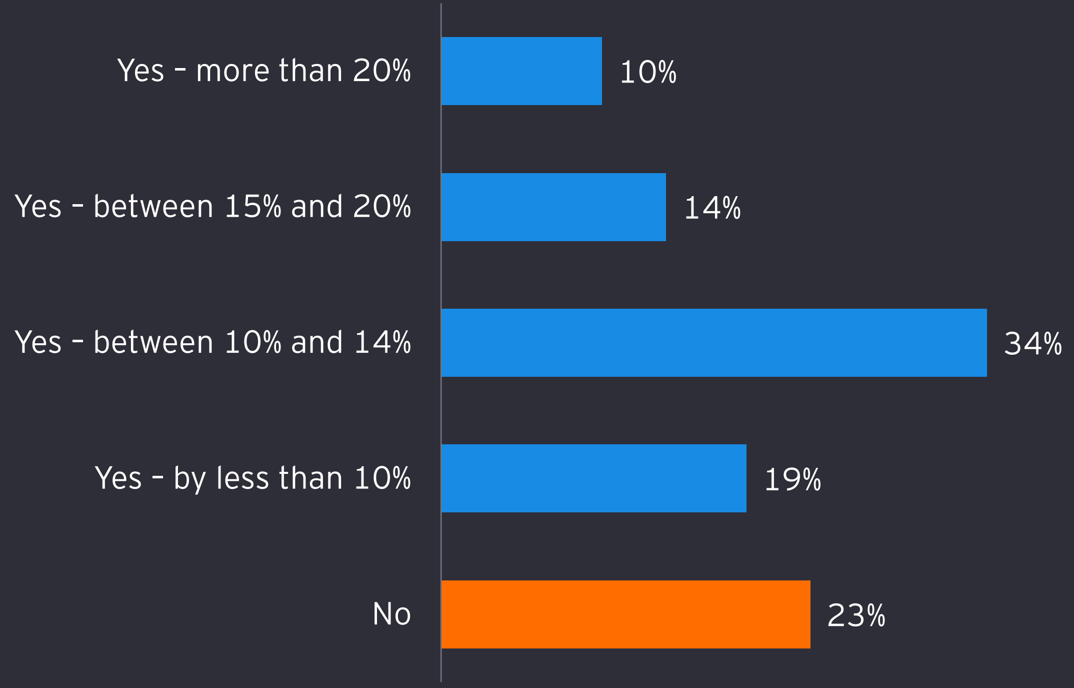
During COVID-19, every business had to adapt to disruption. Progressive organizations rolled out new customer-facing technology that supported remote working and kept the channel to market open.

But the speed of change came with a price. Many businesses did not involve cybersecurity in the decision-making process. New vulnerabilities entered an already fast-moving environment and continue to threaten the business today.

CISOs are worried about vulnerabilities introduced during pandemic-era transformation

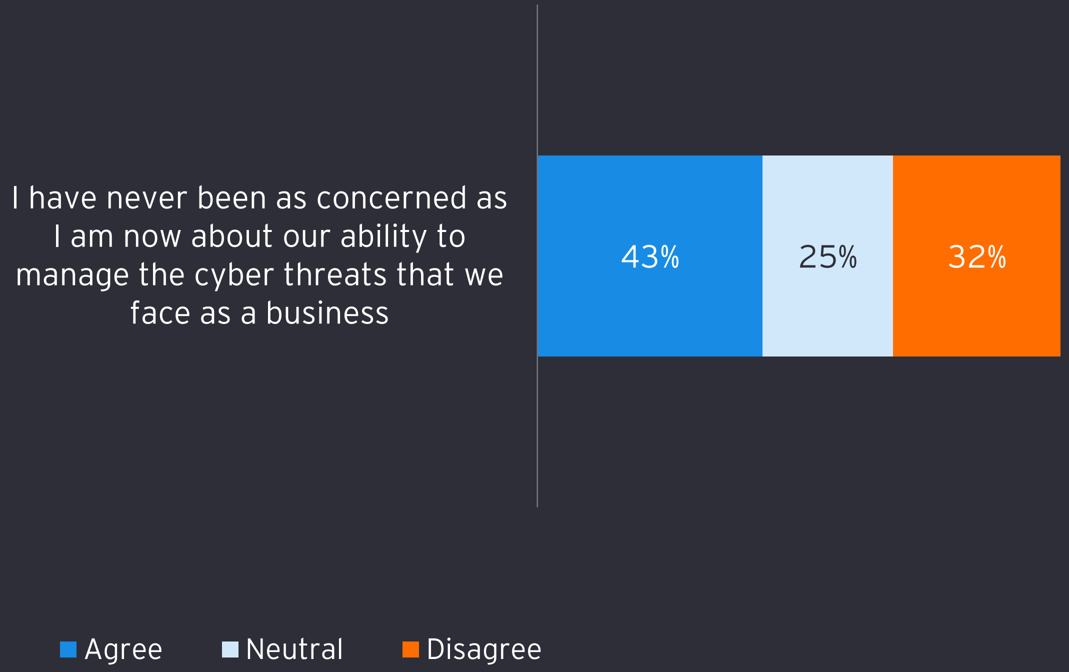
77% of companies saw increases in the number of disruptive attacks. Only 59% saw an increase in 2020.

Q. Have you seen an increase in the number of disruptive attacks over the last 12 months?



43% are more concerned than they have ever been about their company's ability to manage cyber threats.

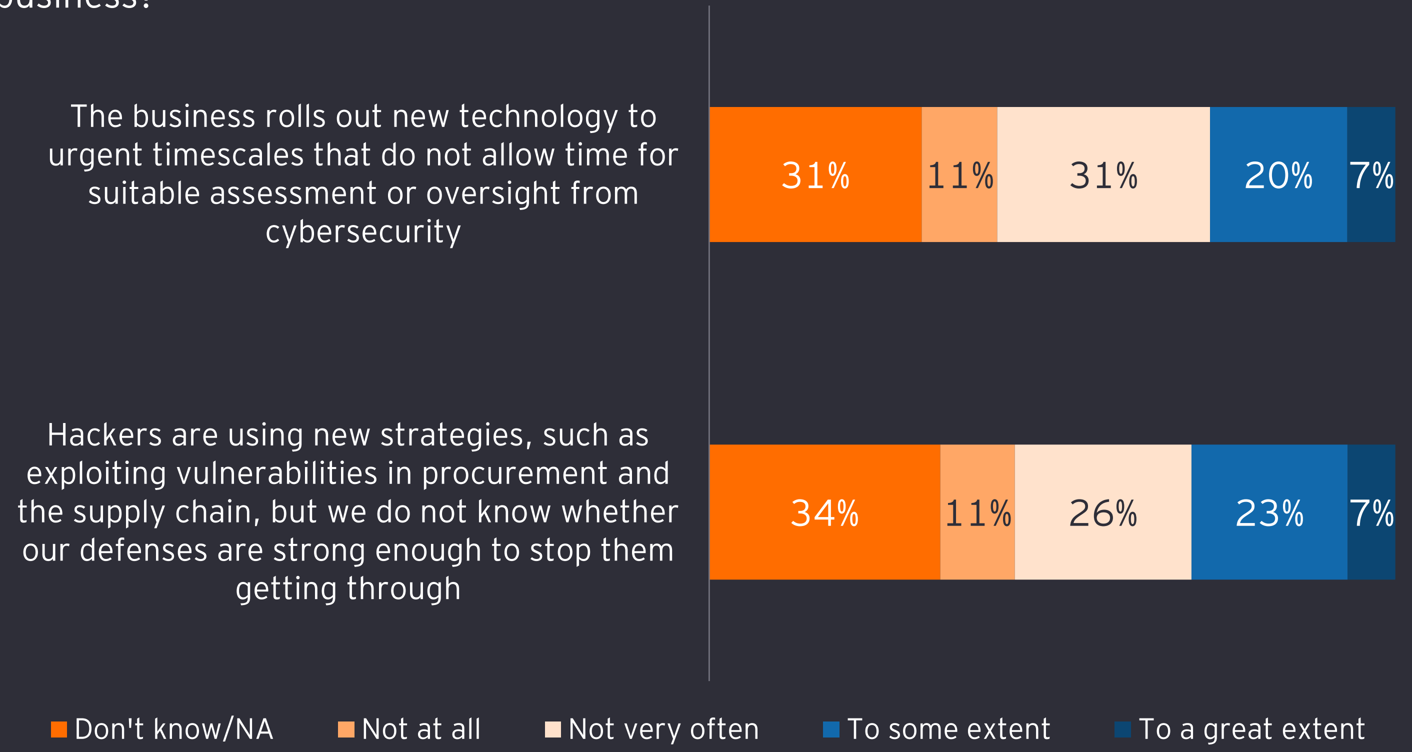
Q. To what extent do you agree with the following statement?



Businesses introduce new technology too quickly for cybersecurity oversight

58% say timescales have been too tight for cybersecurity assessments, and 56% don't always know whether their defenses are strong enough for hackers' new strategies. A lapse only needs to happen once for threat actors to exploit a vulnerability.

Q. How often do the following scenarios take place in your business?



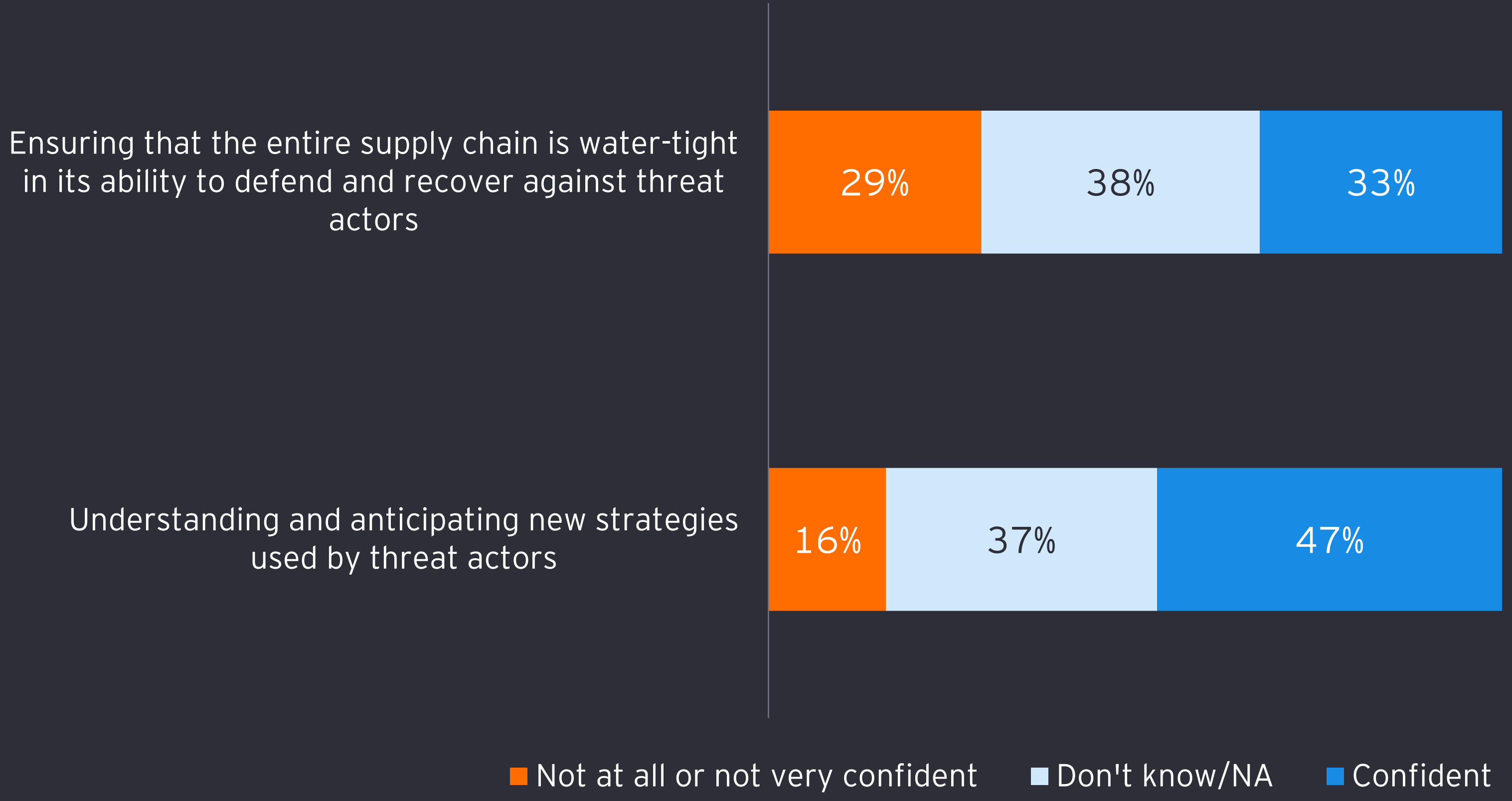
> "There are still organizations that throw projects to security just before they go live.
>
> Richard Watson
>
> EY Asia-Pacific Cybersecurity Risk Consulting Leader

Threat actors have raised their game and are adopting sophisticated new strategies – like using supply chain as the vector of attack

During the last year, hackers have carried out sophisticated and high-profile supply chain attacks.

Today, less than one in three respondents feels confident about making their supply chain fully secure. Less than half can understand and anticipate the new strategies used by threat actors.

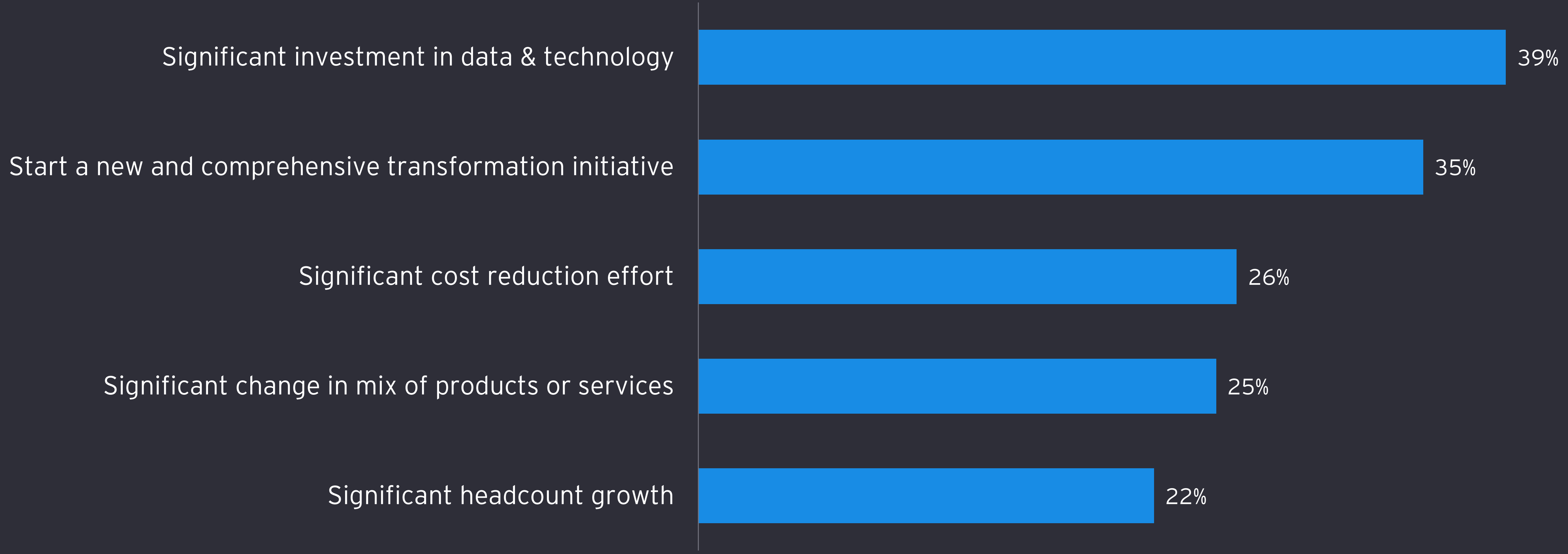
Q. How confident are you in your team's abilities across the following areas?



As businesses continue to pursue new transformation initiatives, the failure to implement security by design will increase risk

Respondents tell us that their businesses are planning a new wave of technology investments, to thrive in the post-COVID-19 era. If cybersecurity is left out of investment discussions, the threat will continue to grow in the years to come.

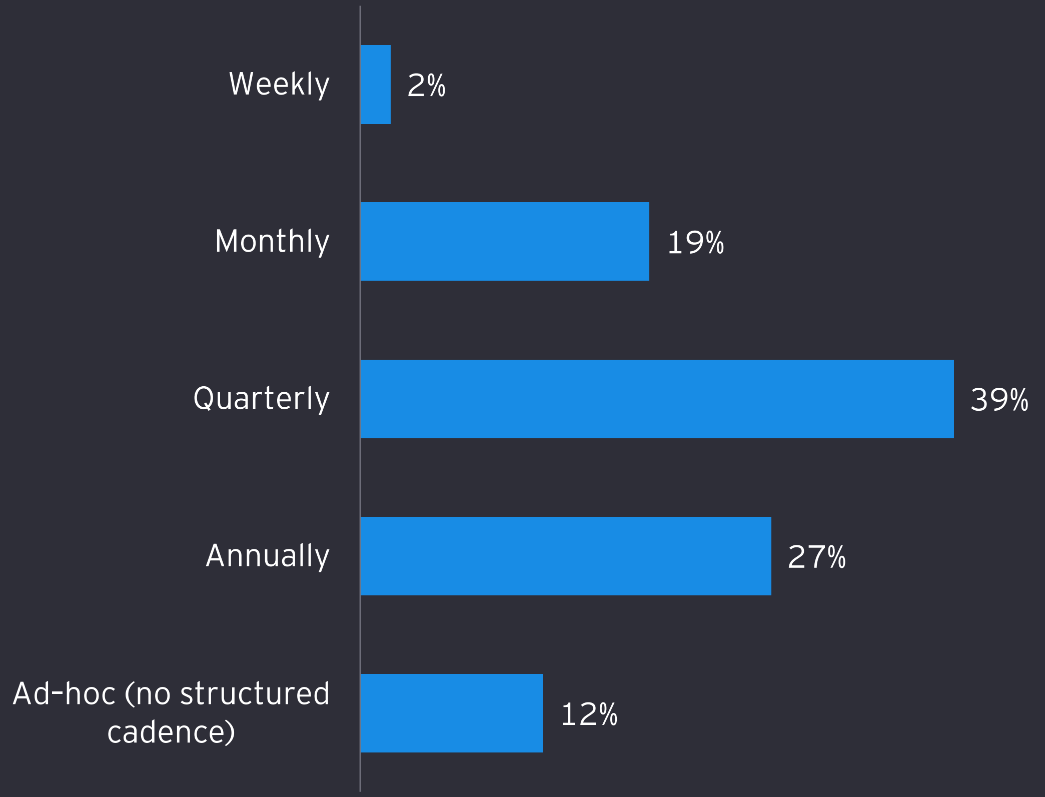
Q. Which of the following actions, if any, do you anticipate your organization will take in the next 12 months?



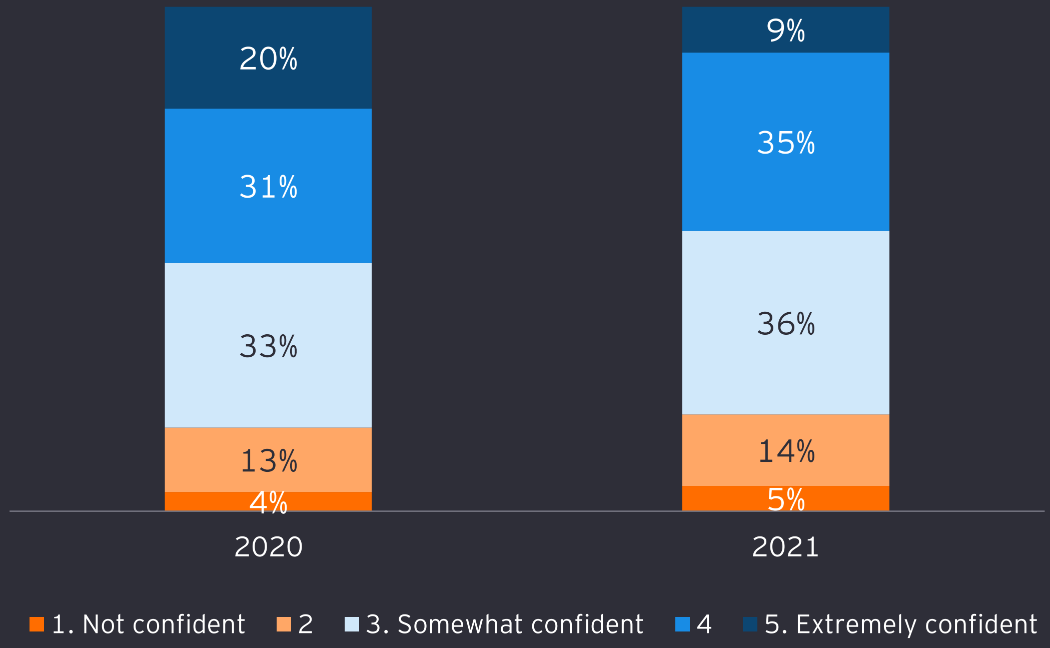
The Board is applying greater scrutiny to cybersecurity

In 2020, 29% said cybersecurity was on the Board agenda quarterly. In 2021, this has risen to 39%. According to the EY *Global Board Risk Survey*, Boards are less likely to be extremely confident in cybersecurity than before.

Q. How often is cybersecurity on the Board agenda?



Q. How confident are you that cybersecurity risk mitigation measures can protect the organization from attacks?*

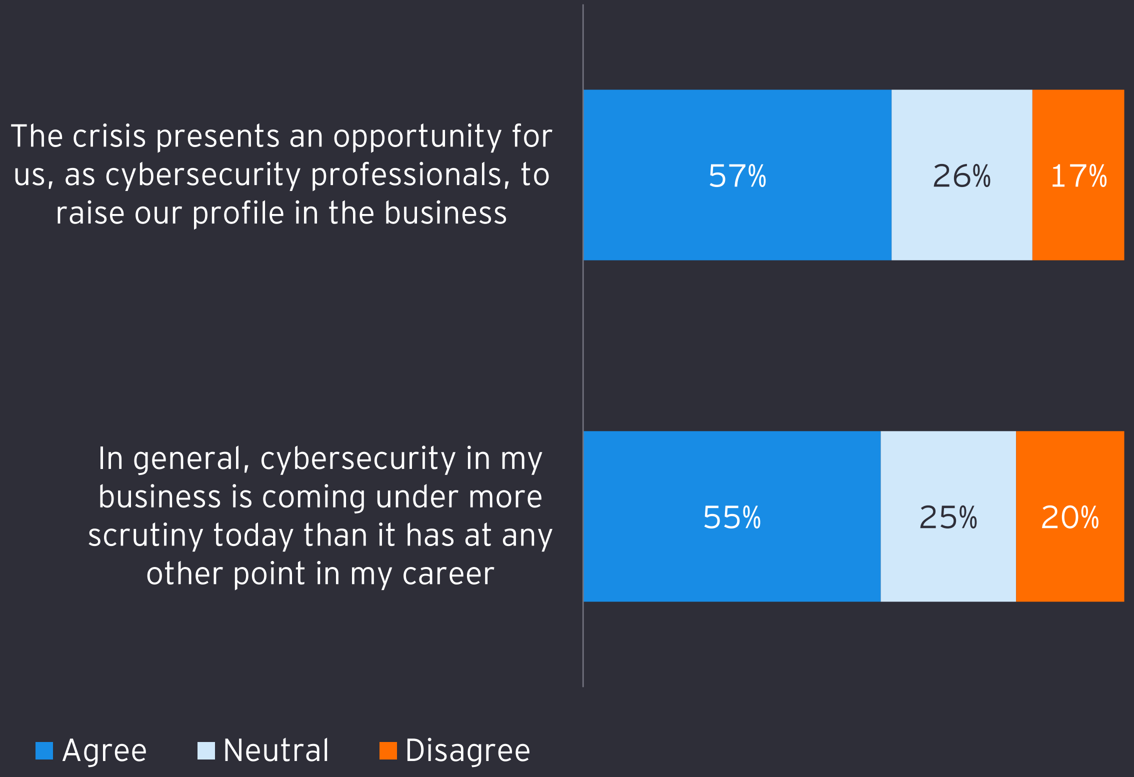


*From the EY Global Board Risk Survey 2021

57% of cybersecurity leaders believe COVID gave them an opportunity to position themselves as strategic partners to the business

At a time when businesses are pursuing new transformation initiatives, the risk of a cyber breach is growing. In turn, CISOs have an opportunity to demonstrate the strategic importance of their role in the post-COVID-19 era.

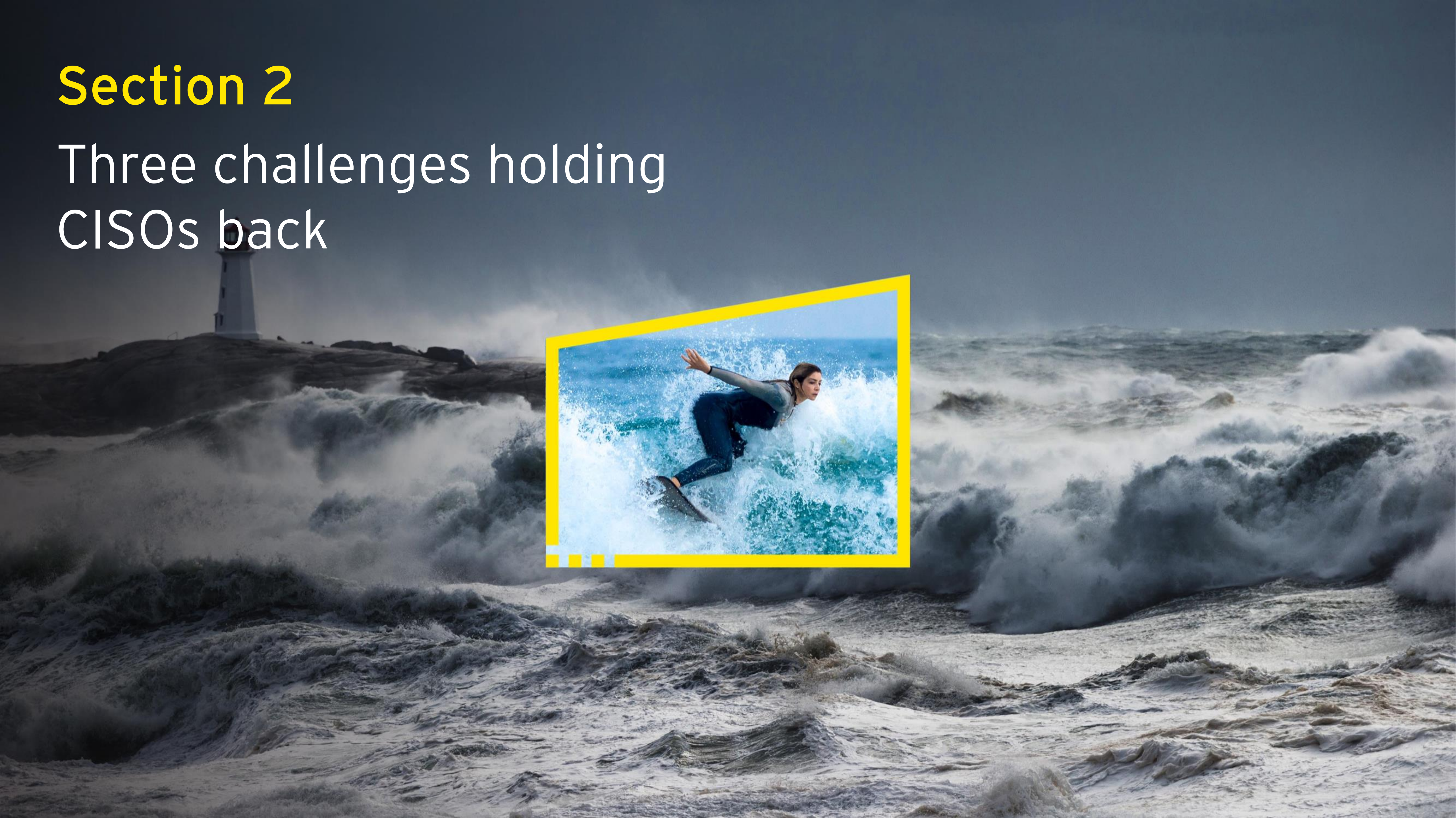
Q. To what extent do you agree or disagree with the following statements?



> “I know of many security officers who were viewed as superstars, and we want those superstars to be brought to the front of innovation.
>
> Dave Burg
> EY Americas Cybersecurity Leader

Section 2

Three challenges holding CISOs back



Three critical cybersecurity challenges

Are CISOs ready to seize the opportunity of a new growth-enabling role?
The answer is yes – but only if they can first address three critical and inter-related challenges:

1 The cybersecurity organization is severely underfunded – but funding is needed more than ever

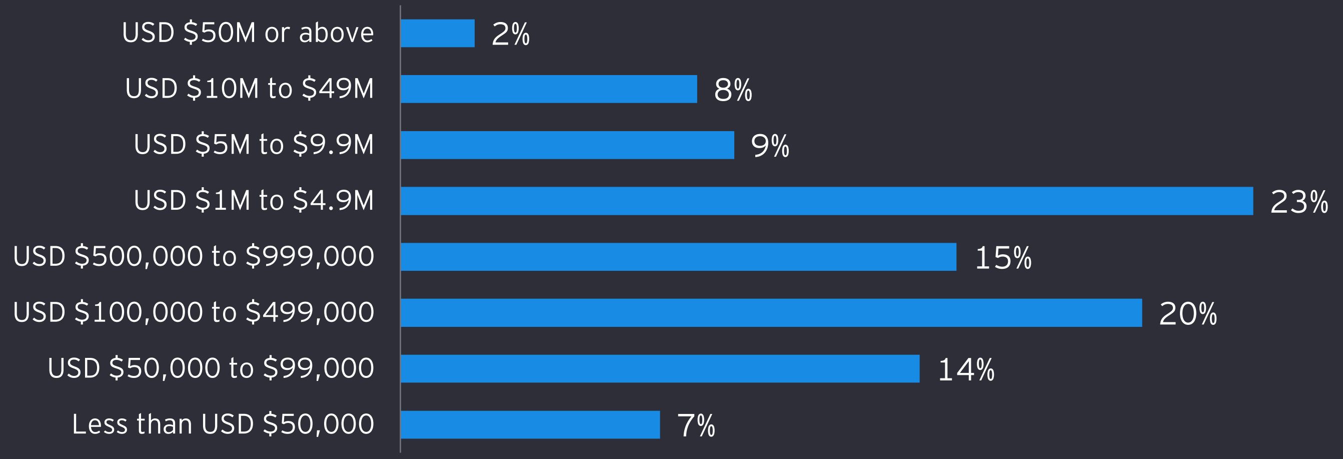
2 Regulatory fragmentation is a headache, creating additional work and resourcing problems

3 CISOs' relationships are weak – when strong connections are key to Security by Design

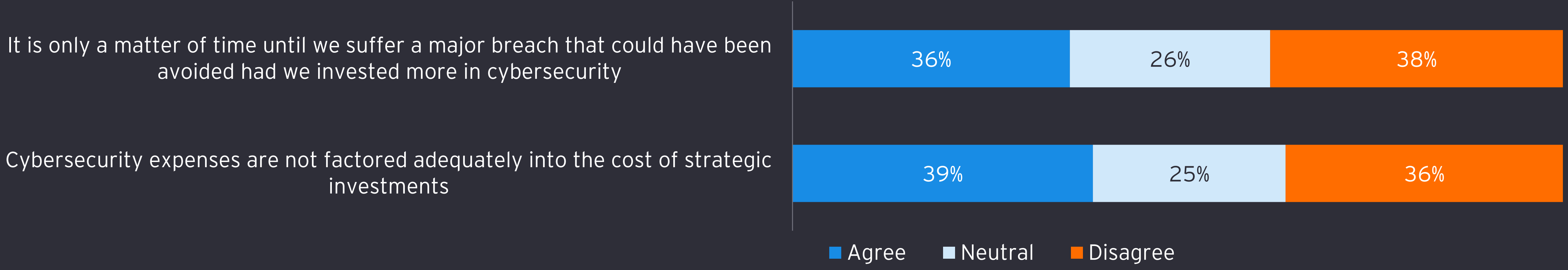
Challenge 1: Today's cybersecurity organization is severely underfunded

Businesses spend between 2 and 5% of annual revenues on IT, according to industry reports. Our GISS research suggests they spend just 0.05% on cyber, on average.

Q. What is your total annual spend on cybersecurity?



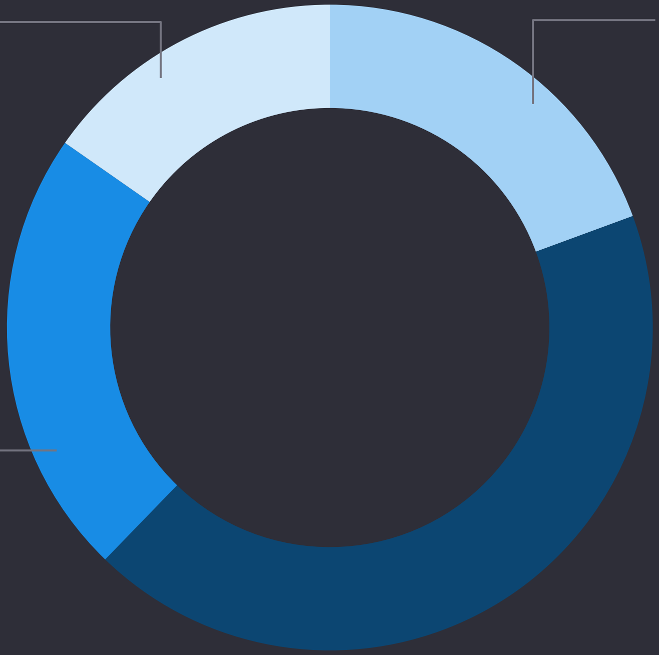
Q. To what extent do you agree with the following statements?



The budget is inflexible at a time when security needs to meet dynamic needs of the business

To support transformation, businesses should consider sharing the cost of cybersecurity across the business. However, just 15% currently do this.

Q. How do you define your cybersecurity budget?



15%

The expense for cybersecurity is shared across business units, which define their contribution dynamically, based on use

19%

The budget is a fixed part of a larger corporate/organizational expense (e.g., 5% of IT/tech) and is defined cyclically

23%

The expense for cybersecurity is a fixed expense, shared across business units, which is defined cyclically

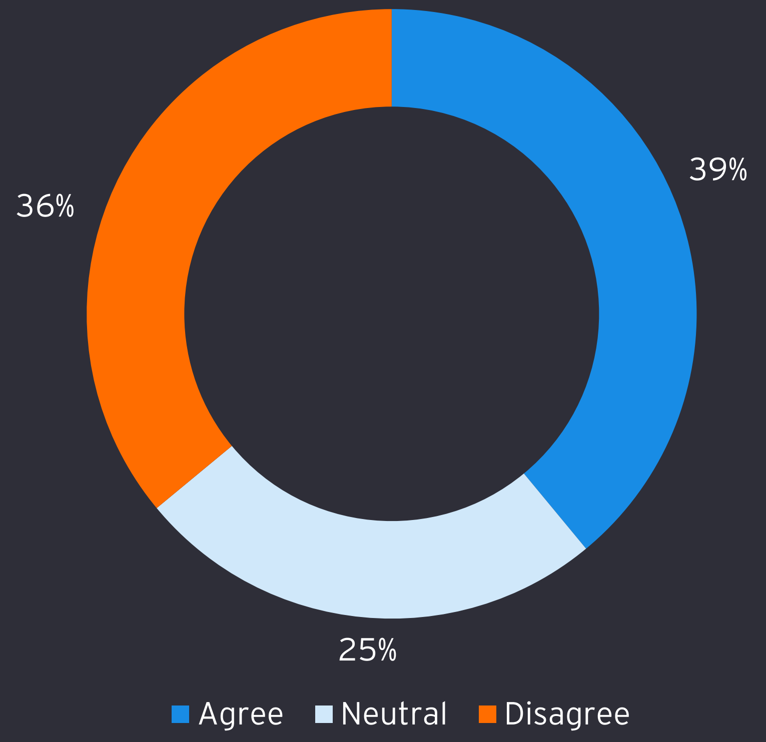
43%

The budget forms part of a larger corporate/organizational expense (e.g., IT/tech) and is defined dynamically

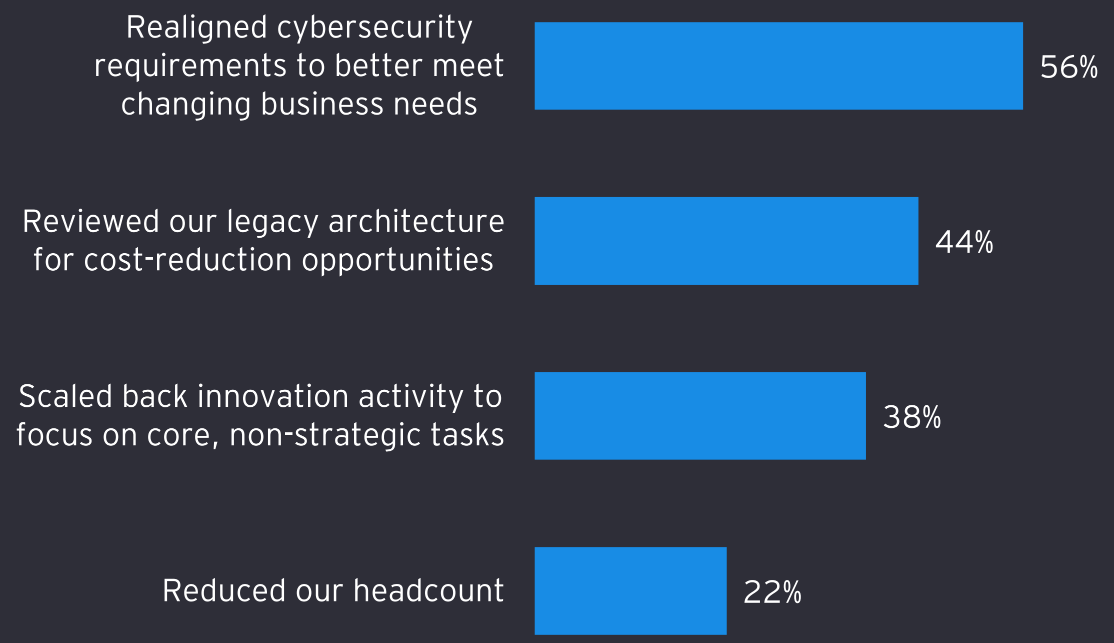
Insufficient budgets are forcing CISOs to make difficult trade-offs between investing in new initiatives vs. addressing existing cyber risk

To cope with budget restrictions, CISOs must make difficult decisions, realigning cybersecurity requirements, and winding down some of the strategic activities that had been put into motion before the crisis began.

Q. "Our budget is lower than we need to manage the challenges that have emerged in the last 12 months"



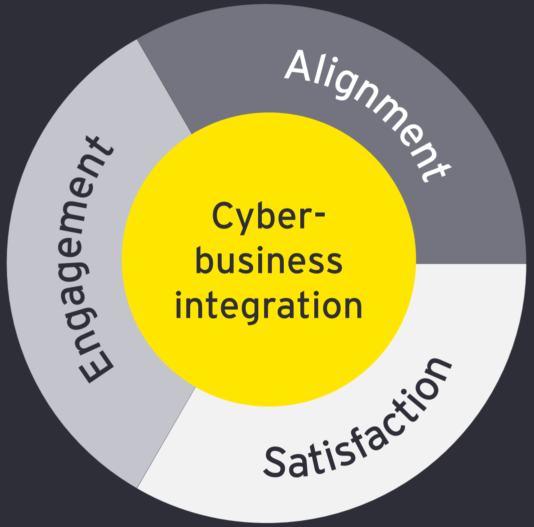
Q. You said your budget was lower than you needed. What actions have you taken to make up the shortfall?



Steps to address the issue: Transform your approach to business alignment

Engagement and communication mechanisms

- Service catalogue with engagement mechanism and cost chargeback
- Communication and governance channels (bi-directional)
- Performance reporting mechanisms



Alignment to business goals

- Map cyber strategy to business and IT strategy
- Establish risk profile to align to business goals and anticipate needs
- Apply appropriate levels of controls to protect the things that matter most

Satisfaction with performance and delivery

- Feedback loops from the business and key stakeholders
- Escalation paths when adjustments and attention is needed
- Recognition for exceptional performance and service

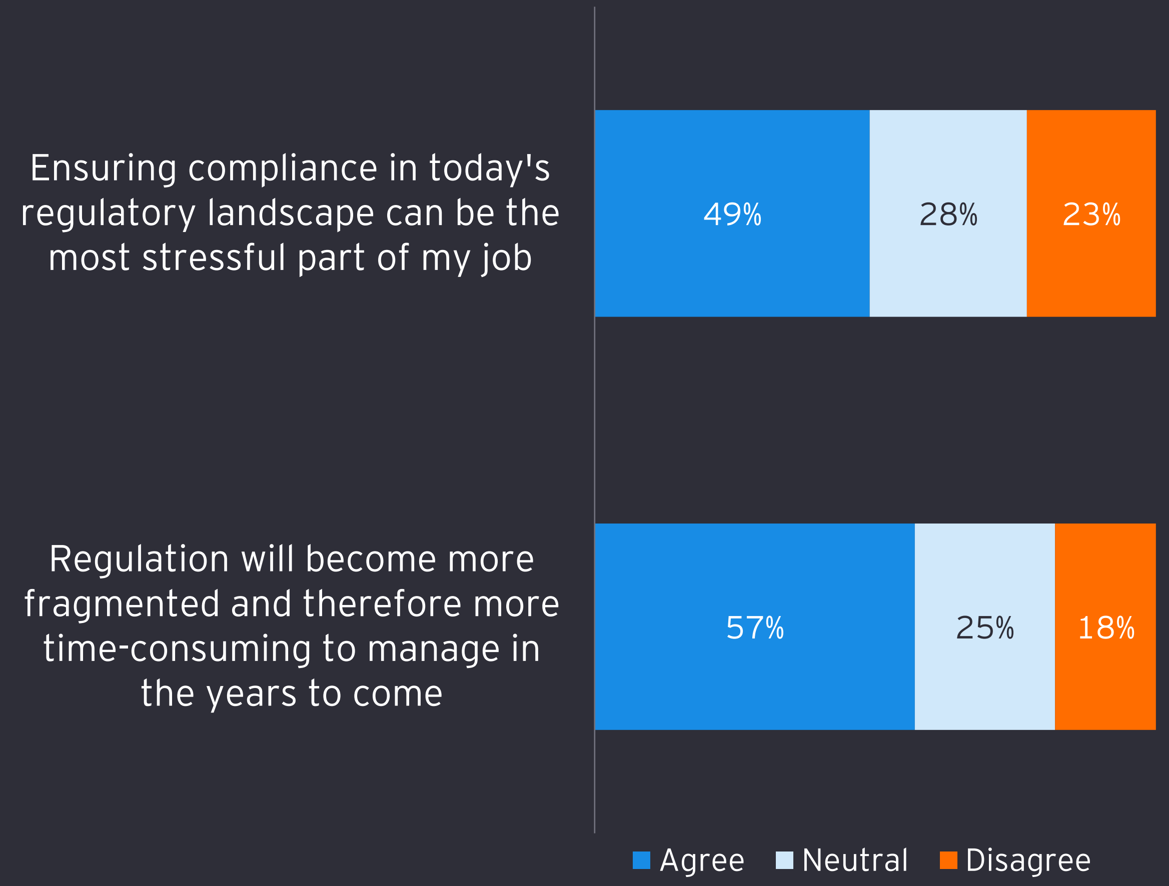
Challenge 2: Regulatory fragmentation is a growing headache for CISOs

The global compliance environment is becoming more complex, with regimes operating at regional and national levels. Organizations in certain sectors must also manage industry-specific regulation. Regulation is claiming time that CISOs do not have to give.

> "If you are an international organization, the way that you manage these overlapping regulations is challenging, particularly as information becomes ubiquitous and travels internationally.

Mike Maddison
EY EMEIA Cybersecurity Consulting Leader

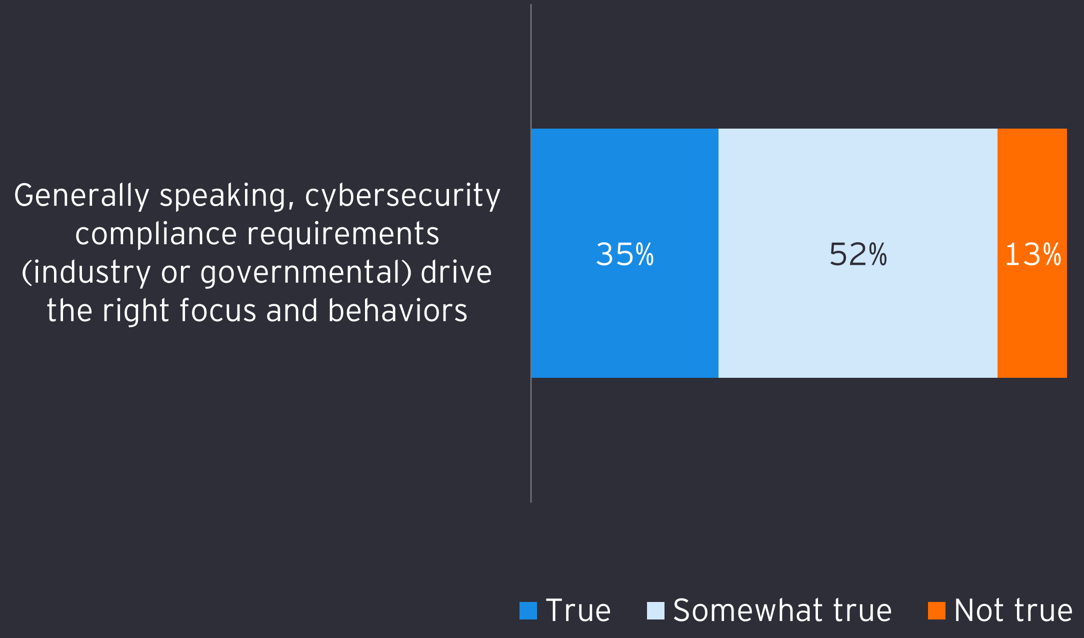
Q. To what extent do you agree with the following statements about regulation?



CISOs are less likely to see the positives in regulation than they were

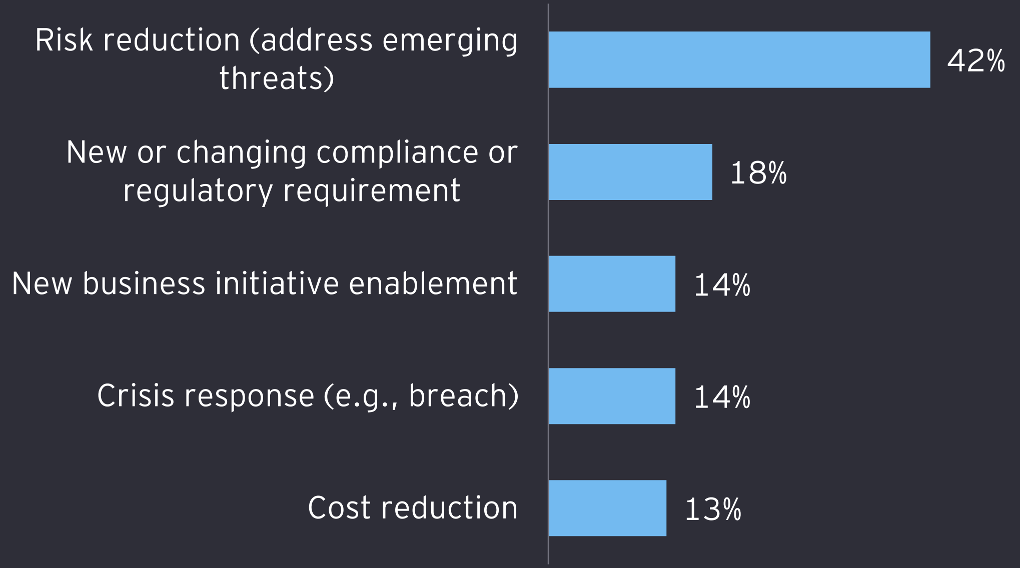
In 2020, 46% of respondents said compliance drove the right behaviors; 5% said this was not true. Their assessment has become more negative over the year.

Q. Is the following statement true?



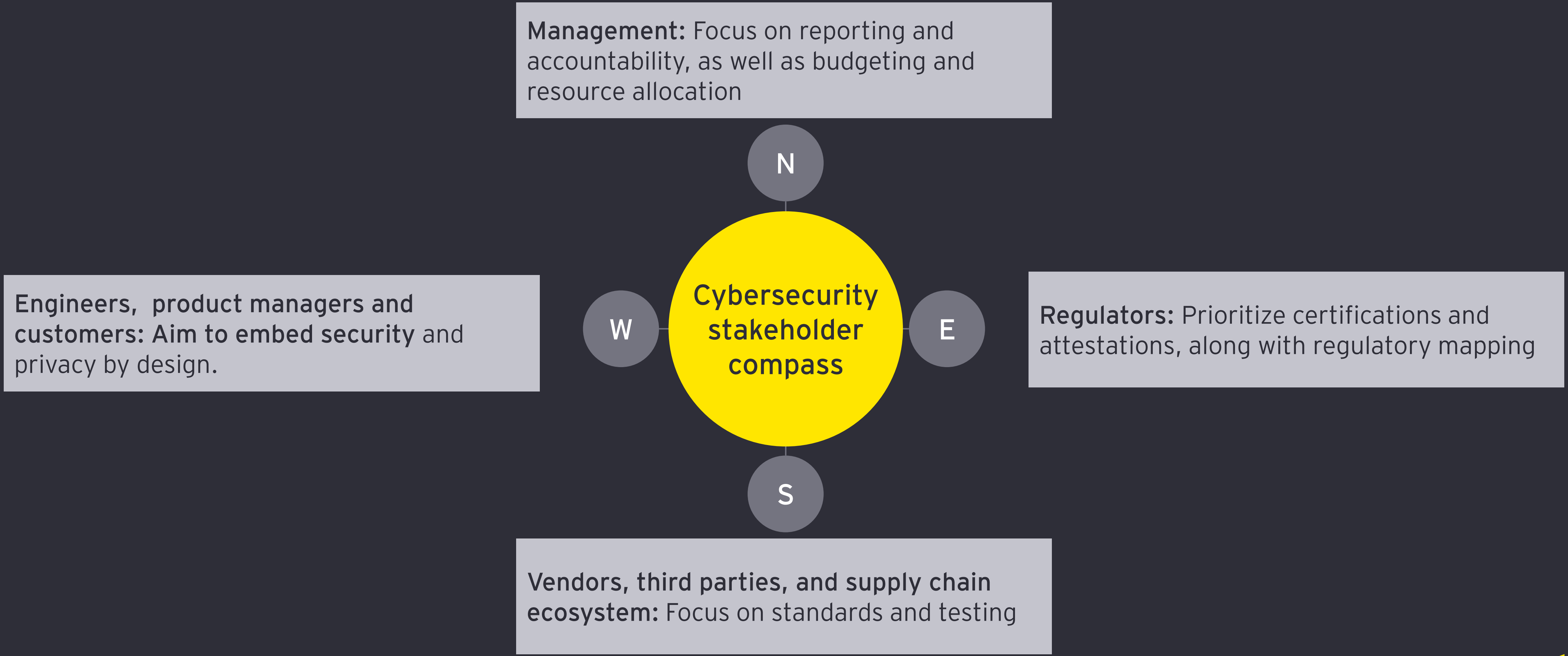
In 2020, 29% described regulation as a primary driver of increased spending. It has since fallen to 18%.

Q. What is the primary driver for new or increased cybersecurity spending?



Steps to address the issue: Understand where compliance sits on a stakeholder compass

CISOs are familiar with the principle of "shifting left," striving to involve cybersecurity earlier on in transformation. Today, they need to understand how to navigate four key stakeholder groups.



Management: Focus on reporting and accountability, as well as budgeting and resource allocation

Regulators: Prioritize certifications and attestations, along with regulatory mapping

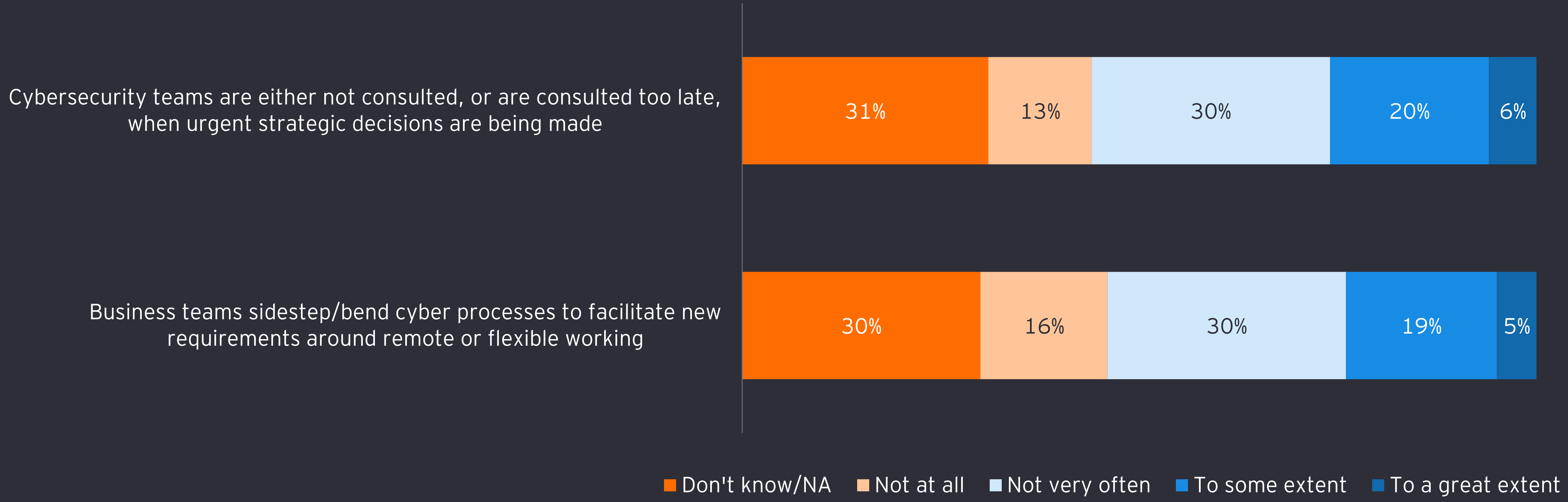
Vendors, third parties, and supply chain ecosystem: Focus on standards and testing

Engineers, product managers and customers: Aim to embed security and privacy by design.

Challenge 3: Cybersecurity's relationships are deteriorating – when healthy relationships are needed the most

CISOs need to provide counsel at the earliest stages of decision-making. But the relationships between cybersecurity and other functions lack positivity and strength. 56% of respondents say cybersecurity teams are not always consulted or briefed in a timely manner. And 54% have seen business teams sidestepping cyber processes to facilitate remote and flexible working. Even if it happens infrequently, it represents a significant risk.

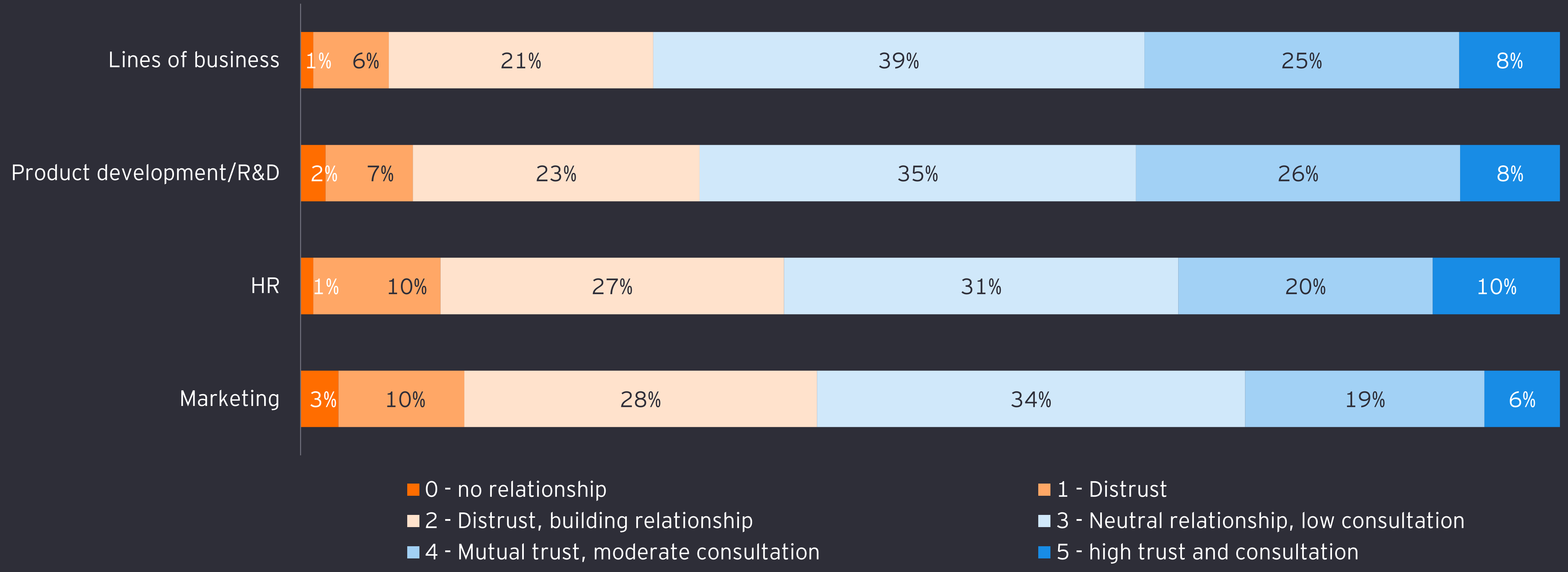
Q. How often do the following scenarios take place in your business?



Cybersecurity relationships with business are characterized by high levels of distrust

Around four in ten say their dealings with marketing and HR are poor. These functions should be working closely with cybersecurity to assess ways of working and new technology.

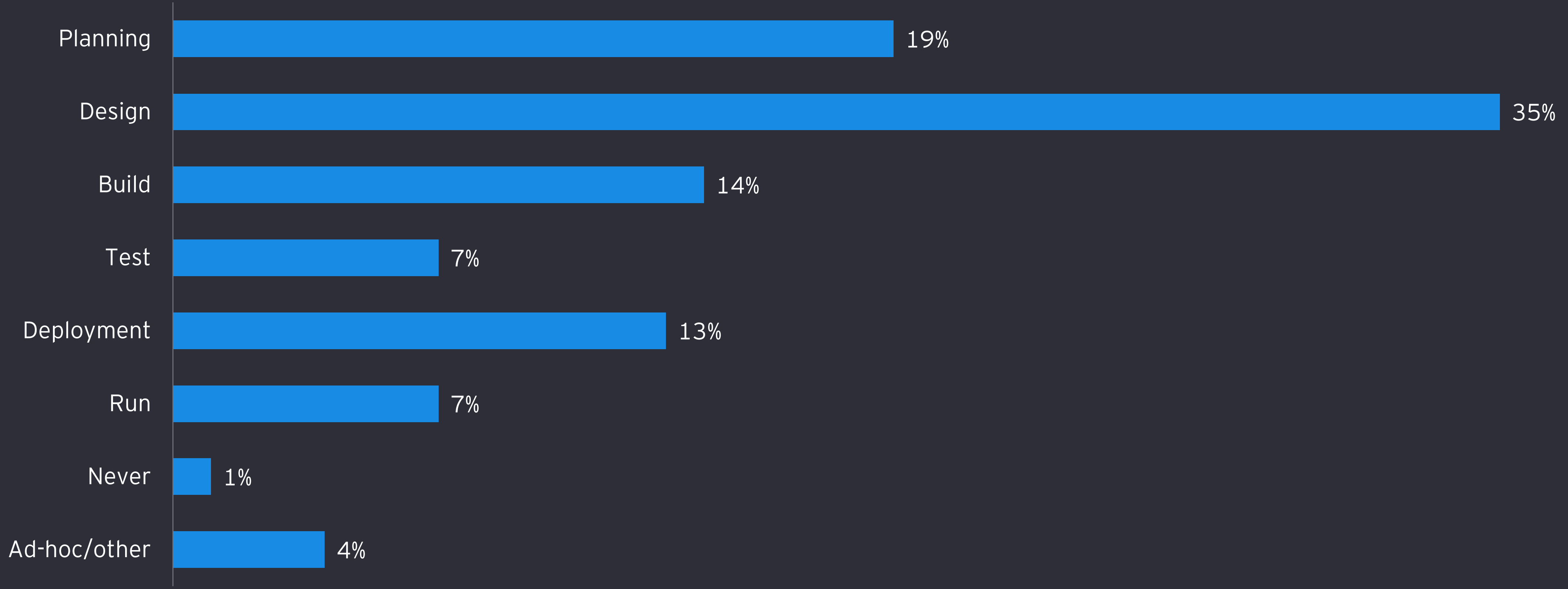
Q. How would you rate the relationship between the Security team and other business functions?



Only 19% of organizations include cybersecurity in the design phase of any digital transformation program

In 2020, 36% said cybersecurity was consulted at the planning stage. This has dropped to 19%. CISOs are now more likely to come in at design (27% in 2020).

Q. At what stage in a new business initiative's journey is the cybersecurity team brought in?

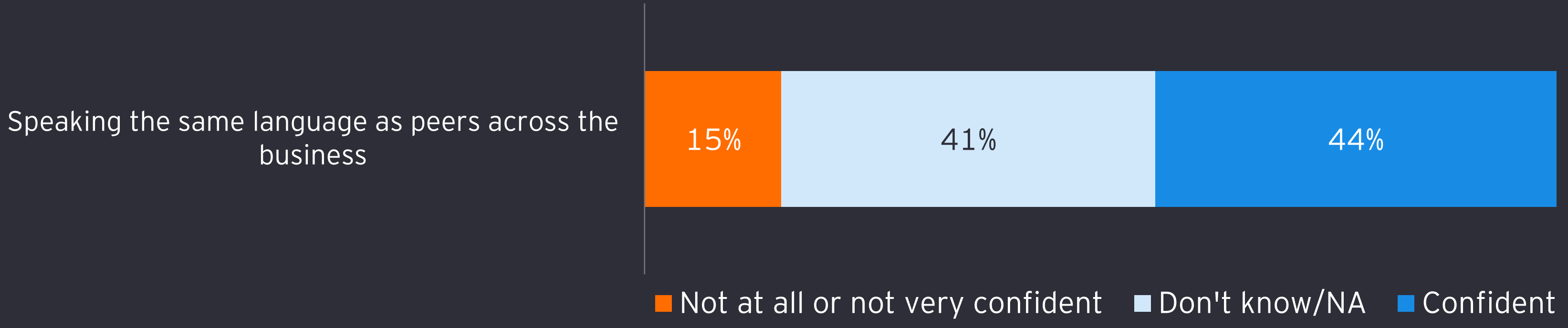


Communication is a growing problem, though the business recognizes core strengths

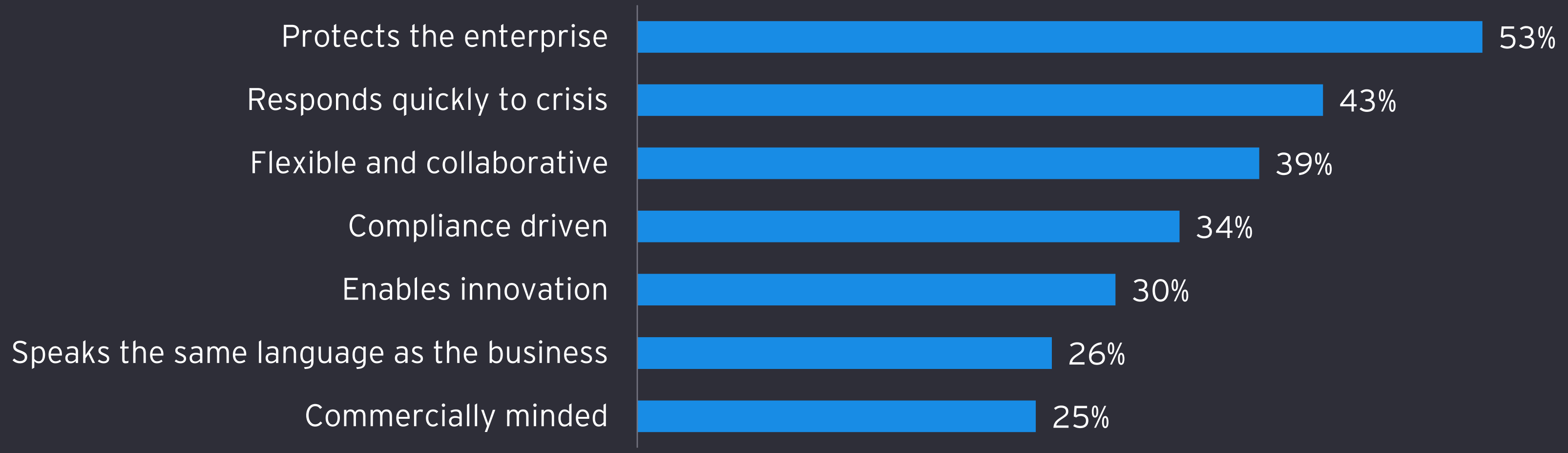
44% of respondents suggest their teams struggle to articulate the need for cyber consultation in commercial terms. Just 29% say they can quantify, in financial terms, how effective their cybersecurity spend is in addressing risk.

Respondents believe that the business recognizes cybersecurity's traditional strengths, such as in controlling risk, but that it does not always perceive cybersecurity as a strategic partner.

Q. How confident are you in your team's abilities across the following areas?



Q. Which terms would executive management use to describe cybersecurity?



Steps to address the issue: Review your talent profile, but don’t expect the impossible

The breadth of skills needed in today’s function is expanding in several directions at once. Here we outline some of the many cybersecurity executive profiles that have emerged in recent years. The best approach is to build a team that balances a combination of broad disciplines, with the understanding that each has its own strengths and weaknesses.

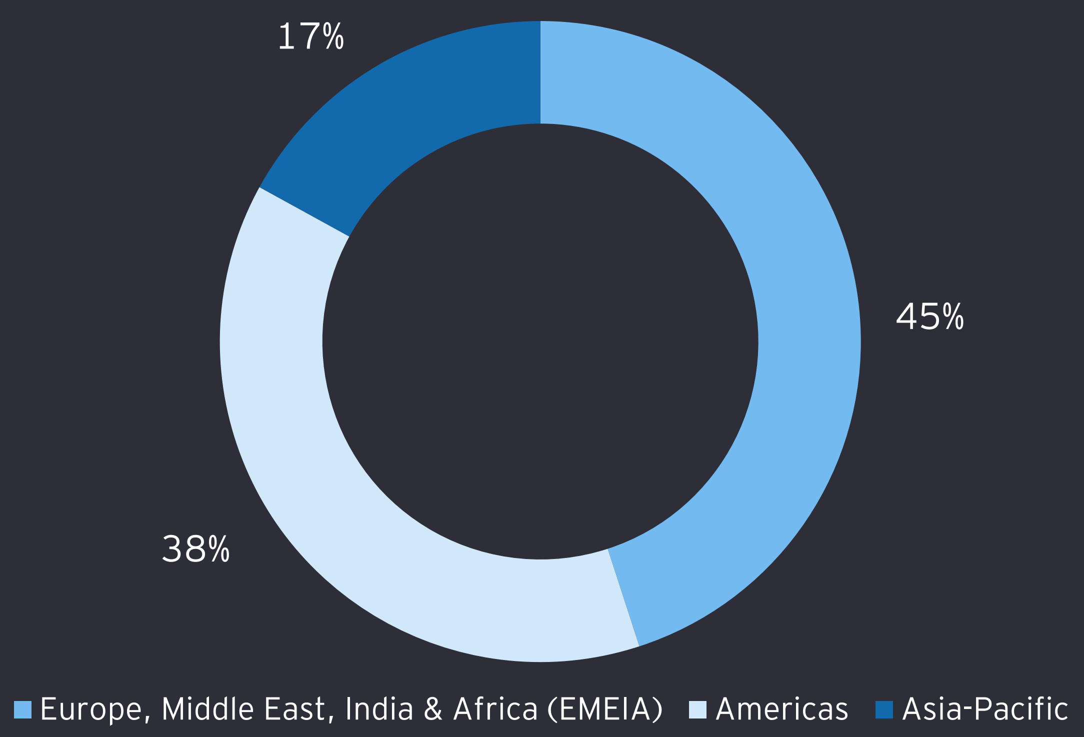
Cybersecurity executive profile	Area of focus	Strengths	Weaknesses
Security expert	All things security	Deep subject-matter expertise	Lack of business acumen
Tech advocate	Technology solutions and tools	Technology oriented	Siloed thinking
Risk and regulatory pros	Risk, controls, and compliance	Good for highly regulated sectors	Lack of technology acumen
Business transplants	Business integration	Business connectivity	Lack of technology and security acumen
Part-timers and job-splitters	Split between cybersecurity and other primary roles	Cost saving	“Jack of all trades, master of none”

Appendix: Demographics

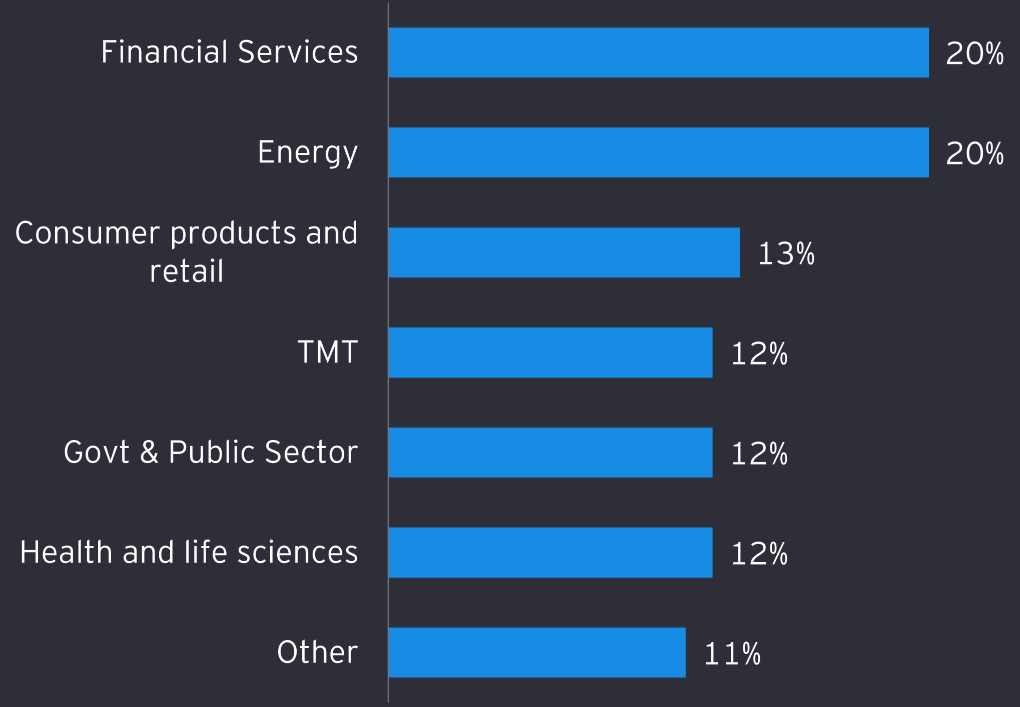
Demographics breakdown

Total number of respondents: 1,430. Total number of $1b+ respondents: 1,010.
Fieldwork took place between March and May 2021, using a mixed methodology of telephone interviews and online surveys

In which region is your company's HQ based?

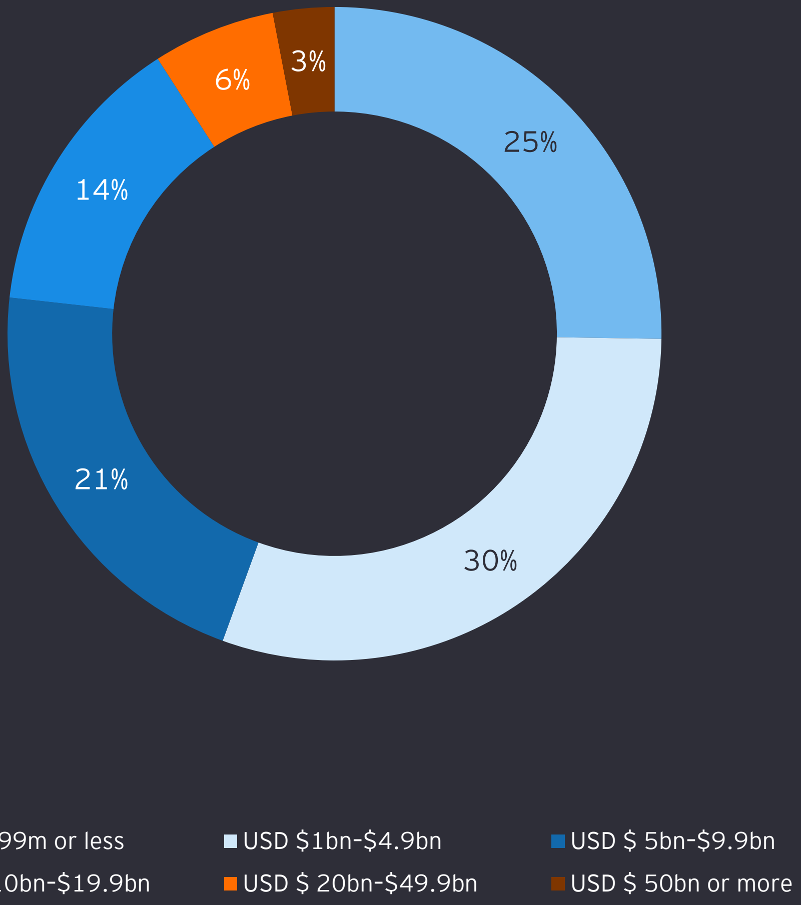


Which industry does your company operate in?

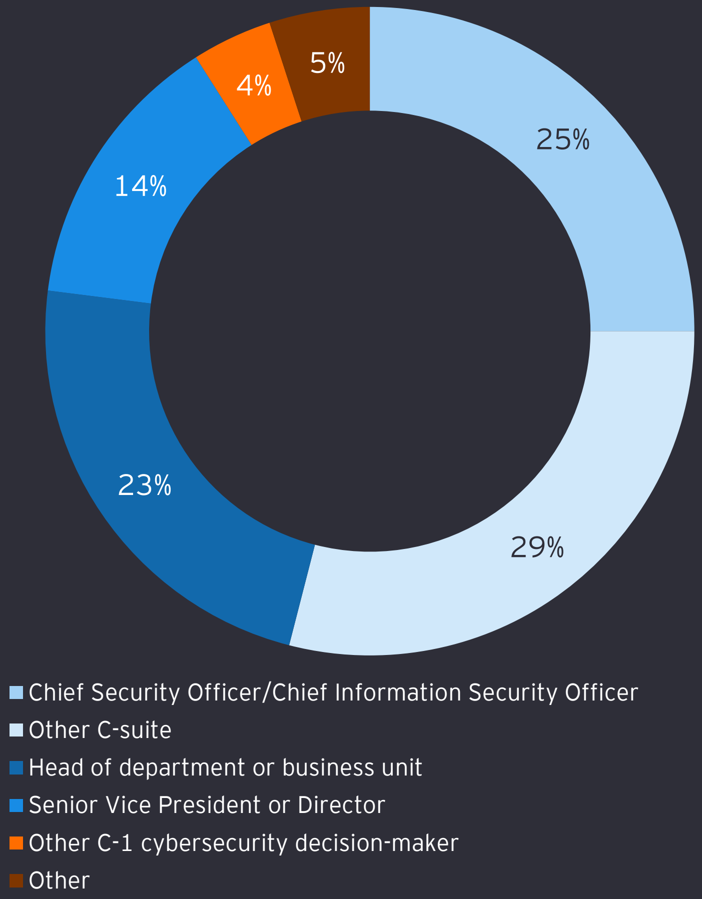


Demographics breakdown

What was your revenue in the last financial year?



What is your job title?

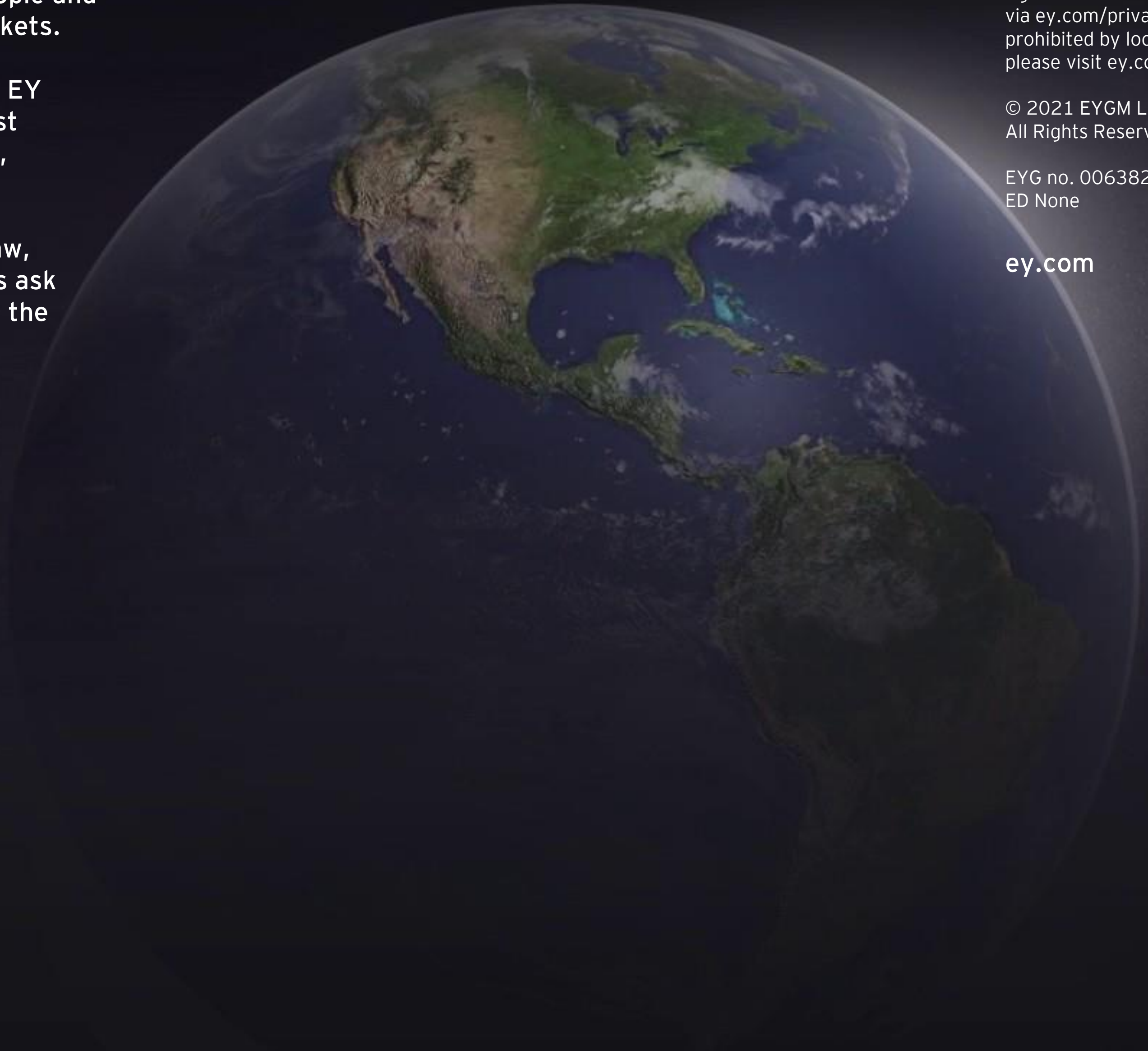


EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



EYG no. 006382-21Gbl
ED None

ey.com