Deloitte.

Insights on Customer Identity & Access Management (CIAM)

Building business value and trust in the Future of Cyber

The link between cybersecurity and business value is growing stronger, according to the fourth edition of *Deloitte Global's Global Future of Cyber Survey*.[1]
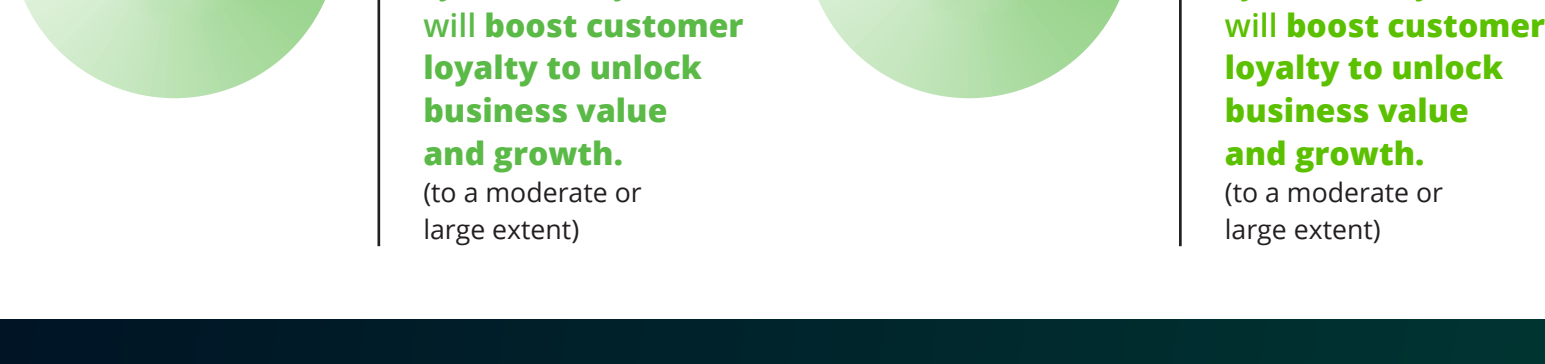
As cyber becomes increasingly integral to driving business outcomes, customer identity and access management (CIAM) has emerged as a critical piece of the value proposition.

Following are some key findings from the survey—insights into how executives are prioritizing CIAM as part of the journey to improve cybersecurity, increase resilience, elevate customer trust, and build a business edge.

INSIGHT 1

Organizations expect significant customer-related outcomes from their cybersecurity initiatives, including those related to CIAM.

Most organizations surveyed anticipate these efforts will lead to increased customer loyalty and business growth.

GLOBAL
85% expect their cybersecurity efforts will **boost customer loyalty to unlock business value and growth.** (to a moderate or large extent)

NORTH AMERICA
90% expect their cybersecurity efforts will **boost customer loyalty to unlock business value and growth.** (to a moderate or large extent)

INSIGHT 2

Organizations with higher levels of cyber maturity[2] tend to have **greater expectations** for customer-related benefits.
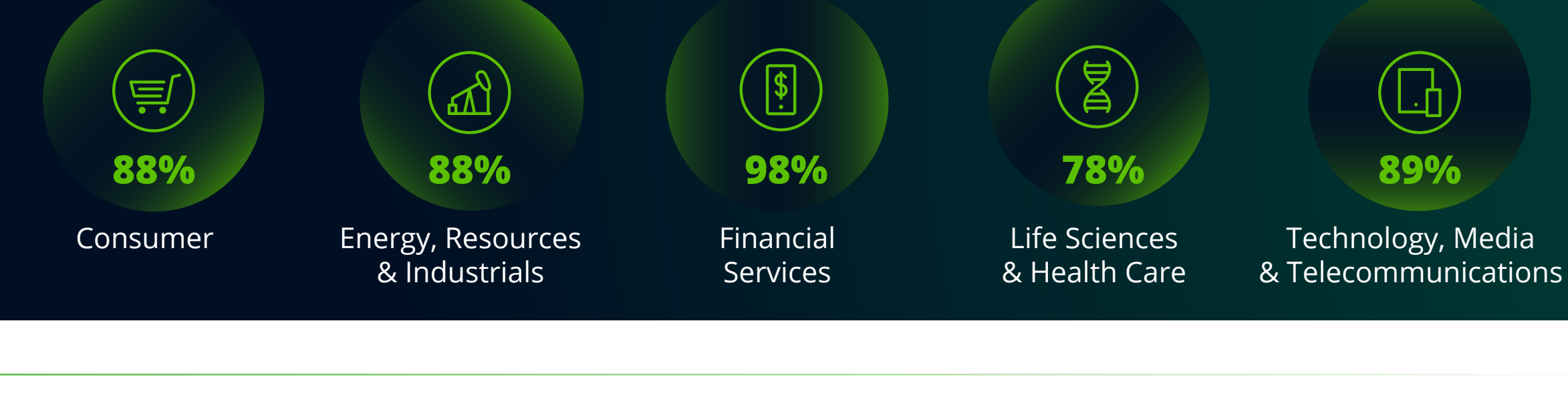
On average, global respondents in high-cyber-maturity organizations are 2.4 times more likely than respondents in low-cyber-maturity organizations (and 1.6 times more likely than respondents in medium-cyber-maturity organizations) to expect positive outcomes from their cybersecurity measures.

CUSTOMER SATISFACTION
70% of high-cyber-maturity organizations are looking forward to improved customer satisfaction and retention. (high cyber maturity)

CUSTOMER LOYALTY
67% expect a boost in customer loyalty to unlock business value and growth. (high cyber maturity)

INSIGHT 3

CIAM is central to cybersecurity and unlocking **business value.**

A large majority of organizations, both globally and in North America, are focusing heavily on CIAM services.

GLOBAL
84% of survey respondents said they were **focused on enhanced controls and measures** to protect customer/ consumer identity and access, and reduce identity fraud. (to a moderate or large extent)

NORTH AMERICA
88% of survey respondents said they were **focused on enhanced controls and measures** to protect customer/ consumer identity and access, and reduce identity fraud. (to a moderate or large extent)

BY INDUSTRY
(US and Canada, to a moderate or large extent)

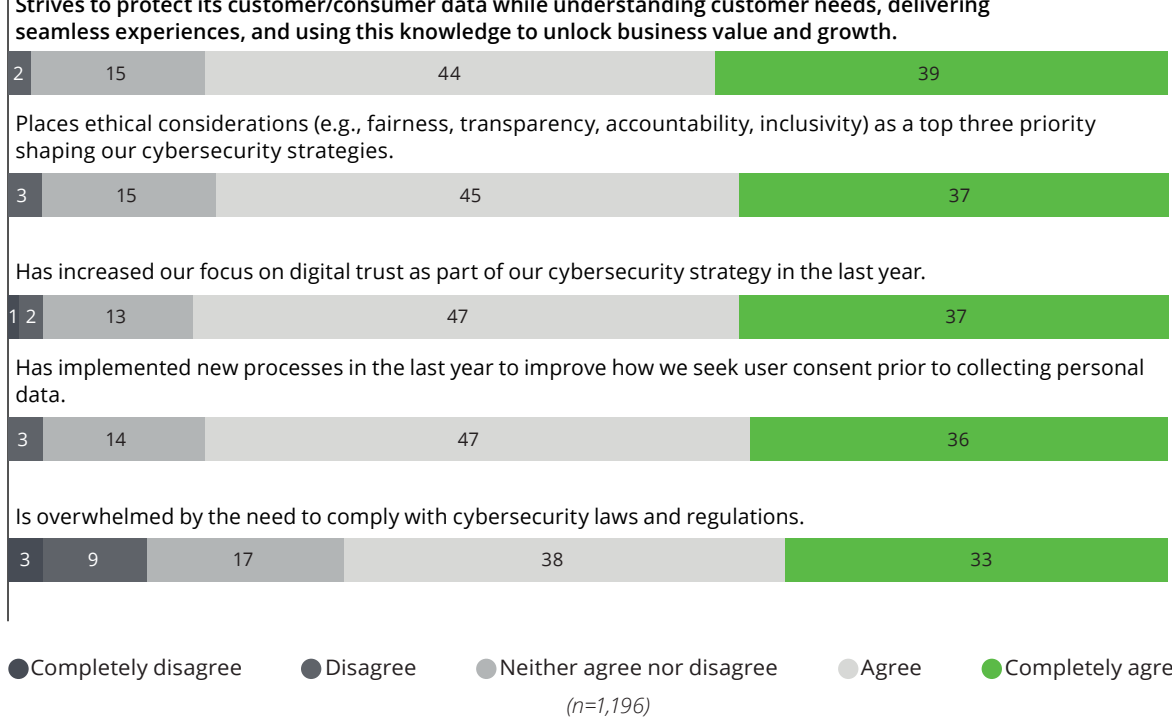| Consumer	Energy, Resources & Industrials	Financial Services	Life Sciences & Health Care	Technology, Media & Telecommunications
88%	88%	98%	78%	89%

INSIGHT 4

CIAM and cybersecurity have become deeply integrated with tech-driven programs and digital business transformation—with **privacy, trust, and ethics** emerging as priorities.

Most global respondents are taking steps to integrate cybersecurity with needs such as product development, protecting customer data, and other key areas.
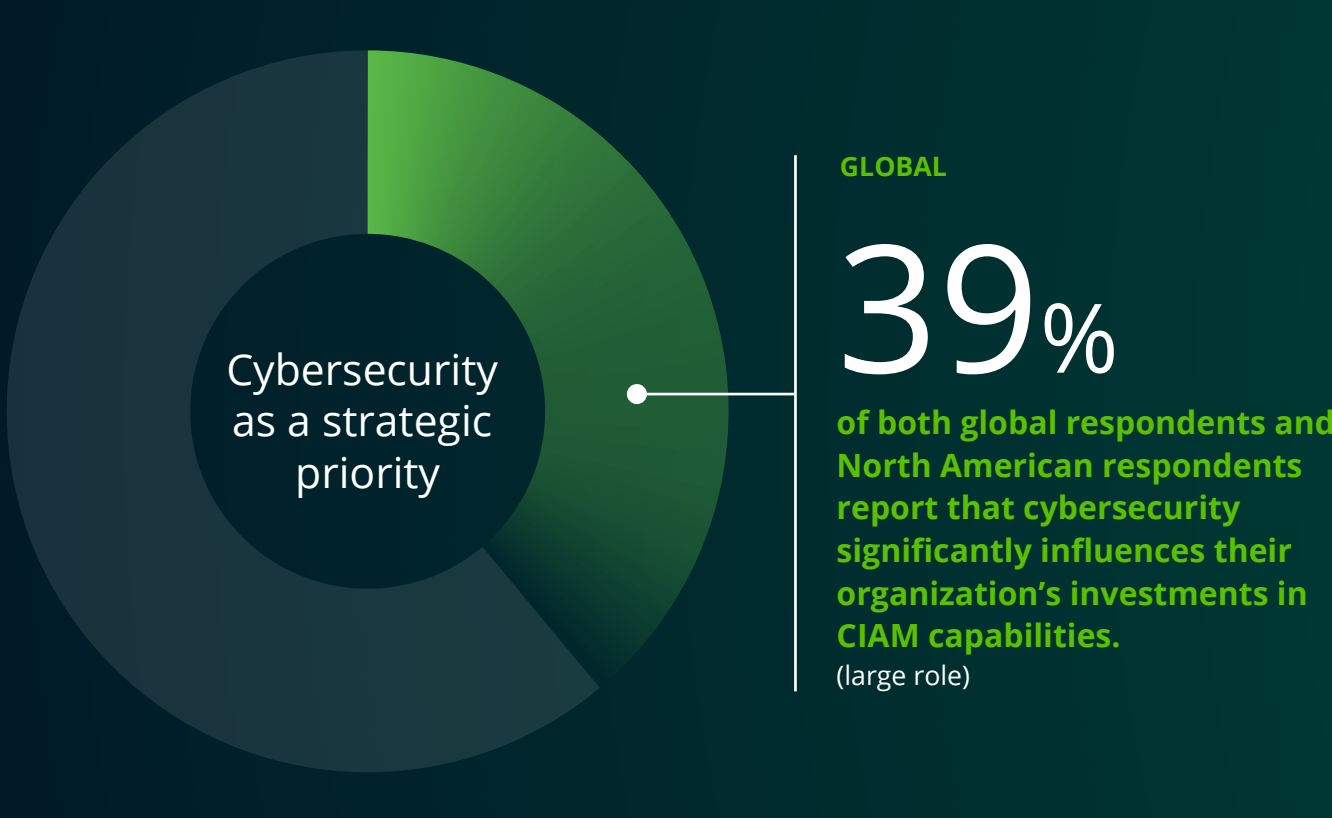
As they pursue technology-driven initiatives and digital transformation, privacy, trust, and ethics have become central priorities for organizations—reflecting a broader commitment to responsible digital business practices.

Among North American respondents, 89% agree or strongly agree that they are striving to protect customer/consumer data while understanding customer needs, delivering seamless experiences, and using this knowledge to unlock business value and growth.

GLOBAL
PRIORITIZING PRIVACY, TRUST, AND ETHICS
(percentage)

Embeds privacy considerations into the initial stages of product or service development.

Strives to protect its customer/consumer data while understanding customer needs, delivering seamless experiences, and using this knowledge to unlock business value and growth.
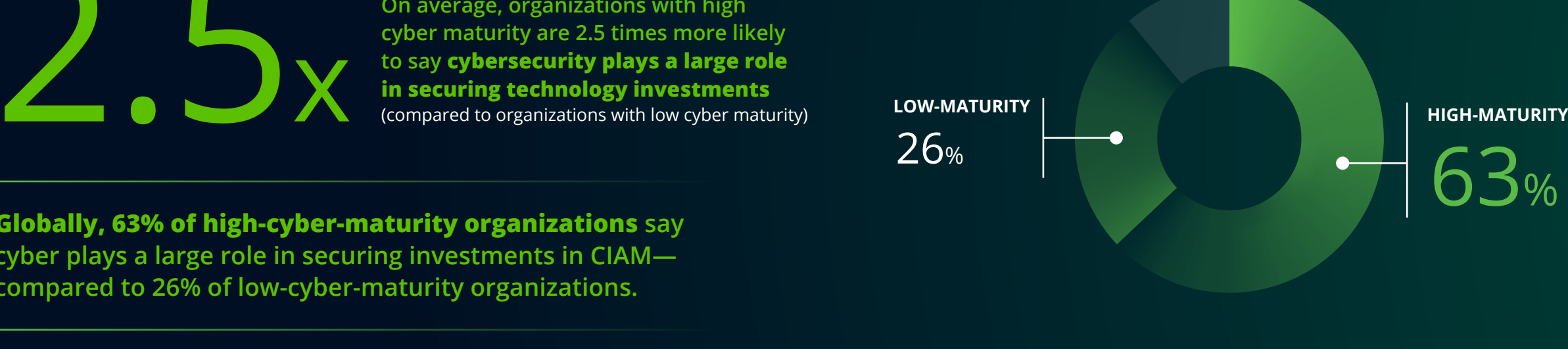
Places ethical considerations (e.g., fairness, transparency, accountability, inclusivity) as a top three priority shaping our cybersecurity strategies.

Has increased our focus on digital trust as part of our cybersecurity strategy in the last year.

Has implemented new processes in the last year to improve how we seek user consent prior to collecting personal data.

Is overwhelmed by the need to comply with cybersecurity laws and regulations.

Completely disagree | Disagree | Neither agree nor disagree | Agree | Completely agree
(n=1,156)

INSIGHT 5

As cybersecurity drives business ambitions, it is also guiding budget allocations for CIAM and other technology capabilities.

Cybersecurity as a strategic priority

GLOBAL
39% of both global respondents and North American respondents report that cybersecurity significantly influences their organization's investments in CIAM capabilities. (large role)
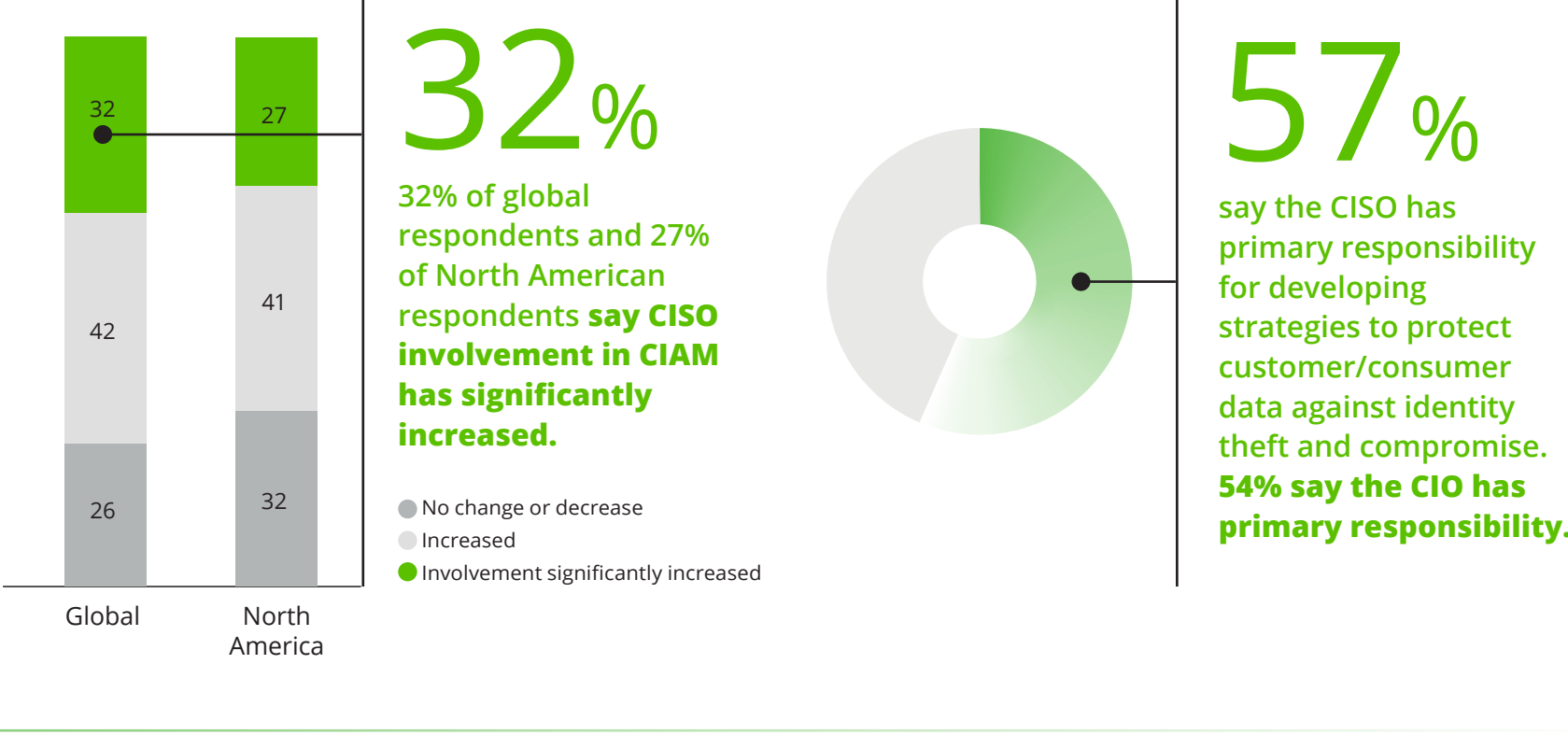

INSIGHT 6

Greater cyber maturity means a greater role for cybersecurity when it comes to **securing investments** in tech-driven capabilities such as CIAM.

2.5x On average, organizations with high cyber maturity are 2.5 times more likely to say **cybersecurity plays a large role in securing technology investments** (compared to organizations with low cyber maturity)

Globally, **63% of high-cyber-maturity organizations** say cyber plays a large role in securing investments in CIAM—compared to 26% of low-cyber-maturity organizations.

LOW-MATURITY 26%
HIGH-MATURITY 63%

INSIGHT 7

The CISO's influence is expanding, with the CISO (or equivalent leader) playing an increasingly active role in strategic business discussions about technology capabilities, including CIAM.

More than two-thirds of respondents (both globally and in North America) say that CISO involvement in CIAM has increased or significantly increased over the past year.

GLOBAL
32% 32% of global respondents and 27% of North American respondents say **CISO involvement in CIAM has significantly increased.**

No change or decrease | Increased | Involvement significantly increased

NORTH AMERICA
57% say the CISO has primary responsibility for developing strategies to protect customer/consumer data against identity theft and compromise. **54% say the CIO has primary responsibility.**

INSIGHT 8

And with increased cyber maturity comes increased CISO involvement in strategic conversations—especially when it comes to capabilities such as CIAM.

GLOBALLY,
52% of high-cyber-maturity organizations say CISOs more frequently are being brought into **strategic conversations about CIAM.**

See the future of CIAM.

Learn more about how the future of cyber is taking shape—and how CIAM is playing a critical role in enabling business resilience and growth.

Contact us to get additional insights.

Contact

Anish Srivastava
Managing Director | Customer Identity
Deloitte & Touche LLP
Email: anisrivastava@deloitte.com

Vikram Kunchala
Principal | Digital Trust & Privacy
Deloitte & Touche LLP
Email: vkunchala@deloitte.com

Anthony Berg
Principal | Identity & Access Management
Deloitte & Touche LLP
Email: antberg@deloitte.com

Additional resources

Global Future of Cyber Survey, 4th Edition | Deloitte Global

Customer Identity & Access Management (CIAM) by Deloitte | Deloitte US

Endnotes

1. The survey asked nearly 1,200 leaders in various industries worldwide to share their views on cyber threats, enterprise activities, and the future.
   To learn more about the survey's methodology, visit deloitte.com/futureofcyber.
2. As part of the global survey, Deloitte Global segmented high-cyber-maturity organizations from their medium- and low-cyber-maturity counterparts.
   See the survey to learn more about the methodology.

Deloitte.

Quick