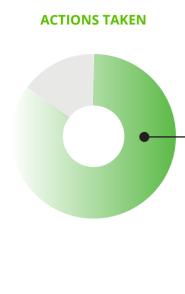
Deloitte. **US FINDINGS FROM** THE GLOBAL FUTURE OF CYBER SURVEY, FOURTH EDITION UNLEASHING THE PROMISE OF CYBER

The link between cybersecurity and business value is growing stronger, according to insights from the fourth edition of Deloitte Global's Future of Cyber Survey.* It asked nearly 1,200 cyber decision-makers across the world, including 203 in the US, to share their views on the evolving cybersecurity landscape and how their organizations are responding.

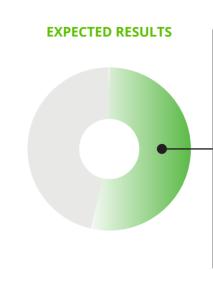
HERE ARE SOME KEY INSIGHTS FROM THE US DECISION-MAKERS SURVEYED...

CYBERSECURITY CONTINUES TO GROW AS AN ESSENTIAL COMPONENT OF THE ENTERPRISE. In addition to cyber strategy being a critical component to unlocking greater business value,

cybersecurity has become increasingly integrated into technology transformation activities.



of respondents are implementing actions to increase cybersecurity (on average, to a moderate or large extent)

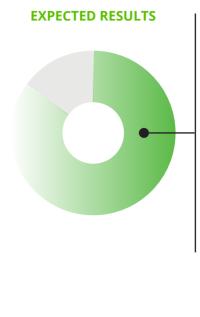


P

Increasing efficiency

and agility

of respondents agree to a large extent that they have a strategic cybersecurity plan with a vision for the future (on average, to a large extent)



of respondents expect to achieve their desired business outcomes as a result of their increased cybersecurity activities (on average, to a moderate or large extent)

cybersecurity initiatives

The top 3 expected outcomes of







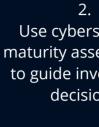
 $\mathcal{V}\mathcal{V}\mathcal{V}$

comprising senior

capabilities and

investments







Protecting

intellectual property

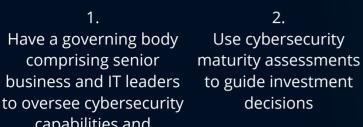
Partner with trusted



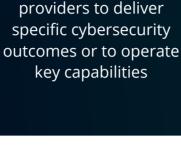
23% Organizations classified as having high

1111









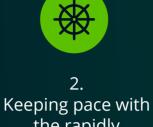


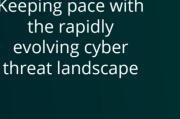
cyber maturity** are more likely to expect to achieve their business outcomes by 23 percentage points versus overall

1.











support from the

C-suite/board

CYBERSECURITY BUDGETS ARE GROWING AND ARE INCREASINGLY INTEGRATED WITH OTHER PROGRAMS.

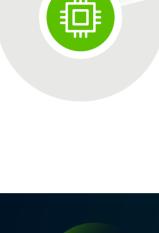


budget over the next 12 to 24 months (4% net increase in budget allocated to cybersecurity) 44% say spend will remain

of respondents

anticipate increasing

their cybersecurity



33% say spend will be prioritized with a budget of its own

of IT budgets are

cybersecurity-related

activities, budgeting

roughly \$19M to \$33M

allocated for

(on average)



of respondents expect to begin integrating cybersecurity spend with budgets for other programs—such as digital transformation initiatives, IT programs, and cloud investments





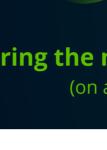
While 41% report that securing the necessary budget is a barrier to their cyber strategy (on average, to a large extent)

THE INFLUENCE OF THE CHIEF INFORMATION SECURITY





siloed and separated





14% say budget ownership will shift from a single owner to multiple



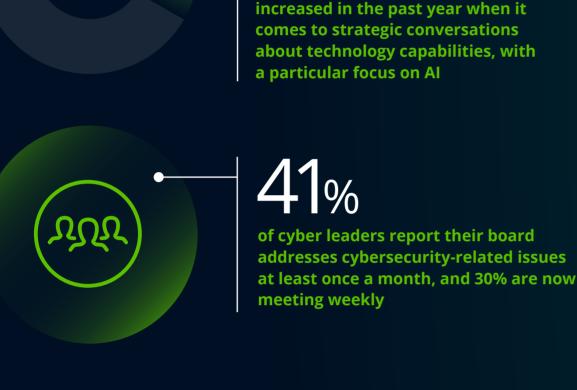
CISO

involvement



of respondents say CISO

involvement has significantly





Respondents who say they Respondents who cited that are very confident in the gaining adequate support C-suite and board's ability from their C-suite and board to adequately navigate is a barrier to their cybersecurity organization's cyber strategy AS THEY SEEK TO AVOID THE IMPACT OF CYBERSECURITY

Top negative consequences reported by respondents in which they have been impacted to a large extent:

INCIDENTS, ORGANIZATIONS' PRIORITIES ARE CHANGING.

Reputational

loss





Intellectual

property theft



50%

Defunding of

strategic initiative



report cyber criminals and terrorists as

for US leaders compared to the overall global benchmark, and nation-states

their leading concerns (with cyber criminals being 7% more of a concern

being 5% less of a concern)

Negative

talent recruitment/

TOP THREAT ACTORS

Almost half of respondents have

reported at least one cyber

breach within the last year.

AI (GENAI) PERSIST.

43%

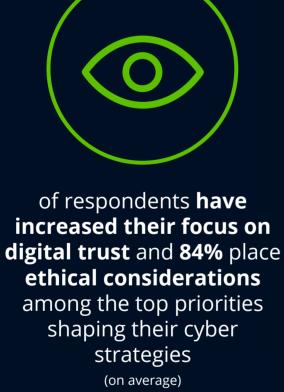
(on average)

92%



ADDITIONAL CONCERNS ARE: of respondents are of their budgets **spent** using AI capabilities in their **on** Al capabilities cybersecurity programs (on average) to a large extent

9%



TECHNOLOGY INVESTMENTS. Percentage of respondents who say cybersecurity plays a large role in securing investment in technology capabilities for... **57**%

MORE IMPACT

Adnan Amjad

Partner

JS Cyber Leade

+1 713 982 4825

+1 408 704 4481

Jennifer Radin **US Cyber Clients** & Industries Leader Deloitte & Touche LLP jradin@deloitte.com

+1 646 420 8350

Deloitte & Touche LLP

aamjad@deloitte.com

31% of respondents are largely concerned when it comes to **Al-related** risks as part of their

cybersecurity strategy

(on average)

49%

about explainability of GenAl ouputs Maintaining privacy and confidentiality of generated outputs

.35%

Social engineering attacks, such as deepfakes Information

integrity risks

of respondents are highly concerned

48%

(on average, compared to organizations with low

Vikram Kunchala

JS Cyber Platform

& Solutions Leader

Deloitte & Touche LLP

Principal

Al

US organizations with high cyber

securing technology investments

maturity** are 2.4 times more likely to

say cybersecurity plays a large role in

Cloud Data analytics

CYBERSECURITY IS KEY TO DRIV

WITH CYBER MATURITY

Explore additional insights from the survey at deloitte.com/global/future-of-cyber Reach out to discuss



Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.



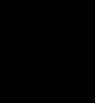
shchand@deloitte.com +1 773 294 6430 **Andrew Morrison** US Cyber Ecosystems & Alliances Leader Principal Deloitte & Touche LLP anmorrison@deloitte.com

+1 404 220 1170

Sharon Chand



vkunchala@deloitte.com +1 713 982 2807 **Kieran Norton** US Cyber Al & Automation Leader Principal



Deloitte & Touche LLP kinorton@deloitte.com +1 415 783 5382

*Find the Global Future of Cyber Survey at <u>deloitte.com/global-future-of-cyber</u>. **Organizations with high cyber maturity are defined as the 14% of US respondents who scored the highest, based on their responses against a set of cyber and AI maturity actions asked about within the survey.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. In addition, this document contains the results of a survey conducted by Deloitte Global. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte.

As used in this publication, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2024 Deloitte Development LLC. All rights reserved.