Global Digital Trust Insights 2024

Studienergebnisse für Deutschland
Oktober 2023

pwc

Inhaltsverzeichnis

Management Summary

1. Höhere Budgets für Cyber Security: 84 % der befragten Unternehmen in Deutschland wollen ihr Budget um mindestens 5 % erhöhen.

2. Cyber Breaches und entsprechende Datenverluste sind deutlich häufiger als in der Vorjahresbefragung – vor allem solche, die Kosten zwischen 100.000 und 1 Million US-Dollar verursachen (2023: 26 %, 2024: 41 %).

3. Die Zukunft ist integriert: 91 % der befragten Unternehmen in Deutschland nutzen bereits integrierte Cyber-Technologie-Plattformen oder planen, diese in den nächsten zwei Jahren zu implementieren, um Cyber Security zu vereinfachen.

4. Die Cloud bleibt ein Sicherheitsrisiko: Unternehmen fürchten Cyberrisiken im Zusammenhang mit Cloud Computing am meisten. Folgerichtig investieren sie in diesem Bereich stark.

5. KI auf dem Vormarsch: In Deutschland planen in den nächsten zwölf Monaten 75 % der Befragten, GenAI-Tools für die Cyberabwehr einzusetzen (global: 69 %).

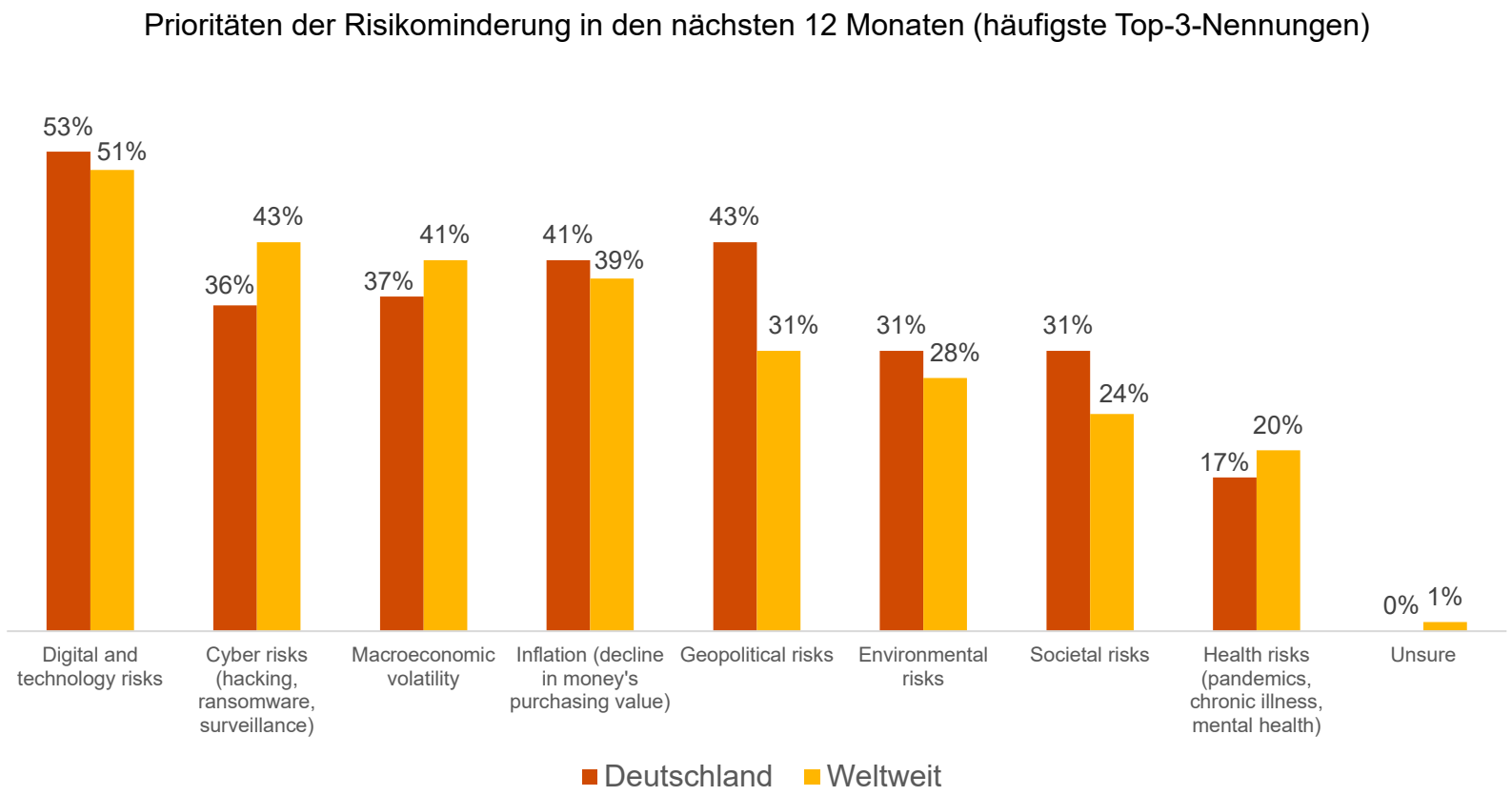
6. Mehr Regulierung erfordert Handeln: Jeweils 38 % der Befragten in Deutschland sehen v.a. die Regulierung von KI sowie Datenschutzbestimmungen als regulatorische Ziele mit großem Einfluss auf das künftige Umsatzwachstum an. In diesem Zusammenhang erwarten sie zunehmende Compliance-Kosten und erhebliche Transformationsbemühungen.

Risikowahrnehmung

Obwohl ein Angriff auf die Cloud zu den größten Sorgen gehört, hat rund ein Drittel der Organisationen keinen Risikomanagementplan für Cloud-Anbieter

pwc

Deutsche Führungskräfte gehen digitale und technologische Risiken mit höchster Priorität an – genau wie ihre internationalen Kolleg:innen



Während Führungskräfte aus der ganzen Welt neben digitalen und technologischen Risken auch Cyberrisiken mit hoher Dringlichkeit mindern wollen, haben in Deutschland geopolitische Risiken eine erhöhte Priorität.

Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top three) Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

Risiken im Zusammenhang mit der Cloud gehören zu den größten Sorgen der Unternehmen in Deutschland und weltweit

52%

Cloud-related threats

Weltweit: 47 %

40%

Attacks on connected devices

Weltweit: 42 %

31%

Business email compromise / account takeovers

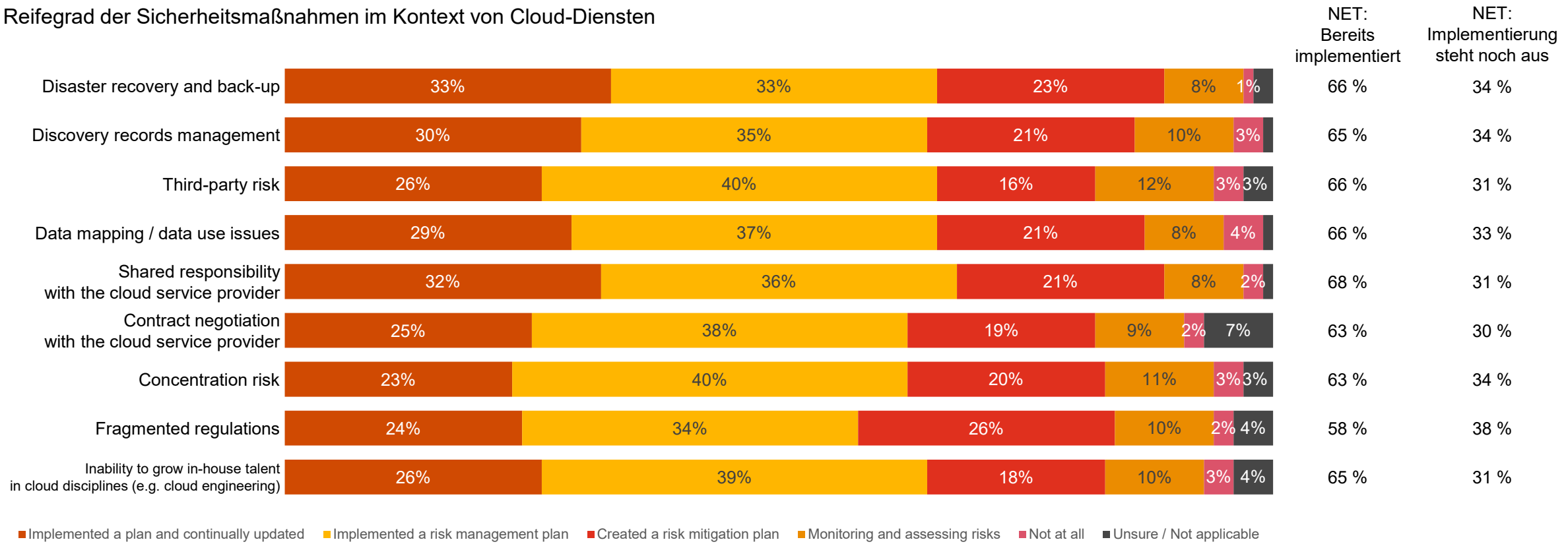
Weltweit: 29 %

> Die weltweit fortschreitende Umstellung auf Cloud-Infrastrukturen sorgt dafür, dass das Bewusstsein für entsprechende Risiken in den Führungsebenen wächst.
>
> Aleksei Resetko, Partner Cyber Security & Privacy bei PwC Deutschland

Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three) Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

Ein erheblicher Anteil der Unternehmen hat noch keinen Risikomanagementplan für Herausforderungen im Zusammenhang mit Cloud-Anbietern eingeführt

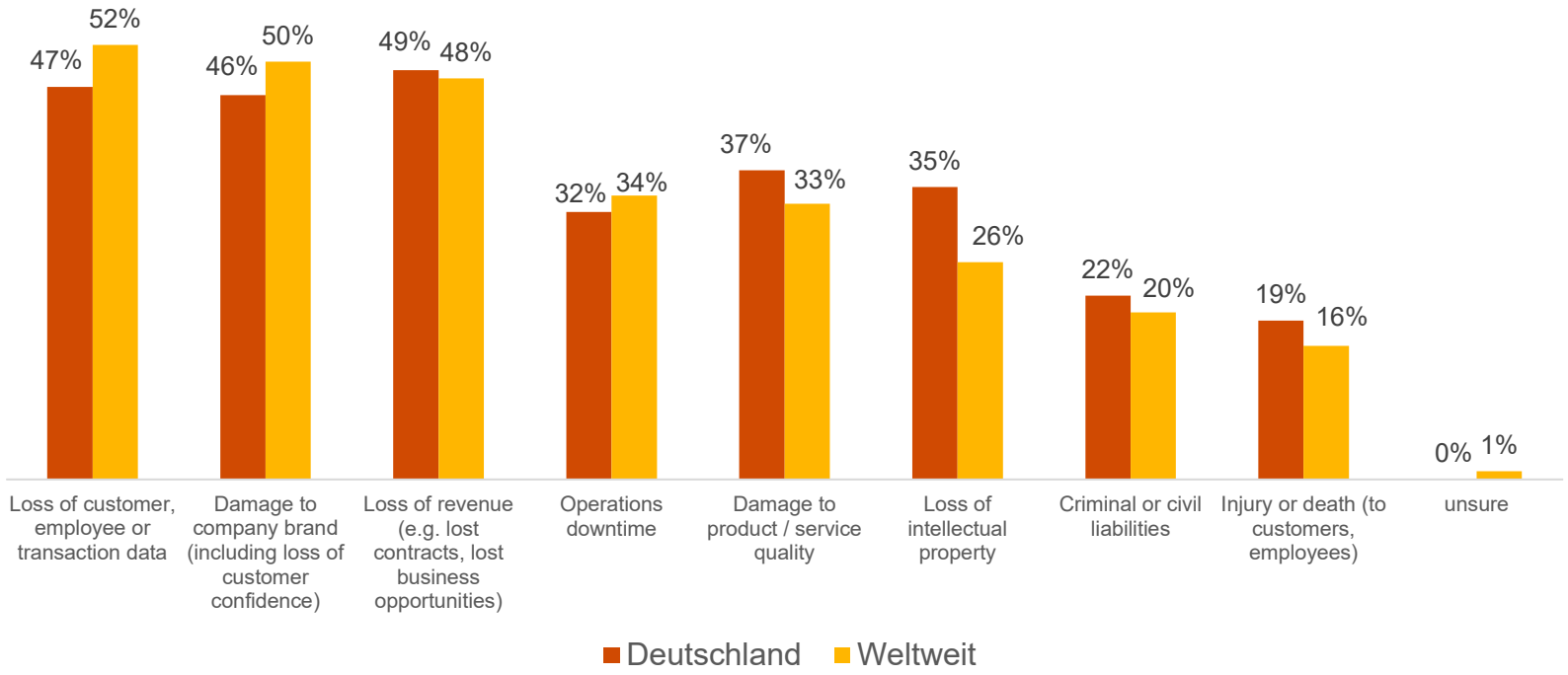


Q19. To what extent has your organisation addressed the following challenges with your cloud service provider(s)? Base: Germany=257

Source: PwC Digital Trust Insights 2024

Größte Sorgen: Verlust von Daten von Kunden und Mitarbeitenden, Umsätzen sowie Reputationsschäden

Größte Sorgen der Unternehmen in Hinblick auf die Folgen eines möglichen Cyberangriffs in den nächsten 12 Monaten (häufigste Top-3-Nennungen)



Datenverluste, Umsatzeinbußen und Reputationsschäden gehen im Falle von Cyberangriffen oft unmittelbar Hand in Hand. Aus diesem Grund werden die Risiken sowohl in Deutschland als auch global gleichermaßen gefürchtet.

Grant Waterfall, Partner sowie Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

Q4. Over the next 12 months, which of the following potential outcomes of cyber attacks is your organisation most concerned about? (Ranked in top three) Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

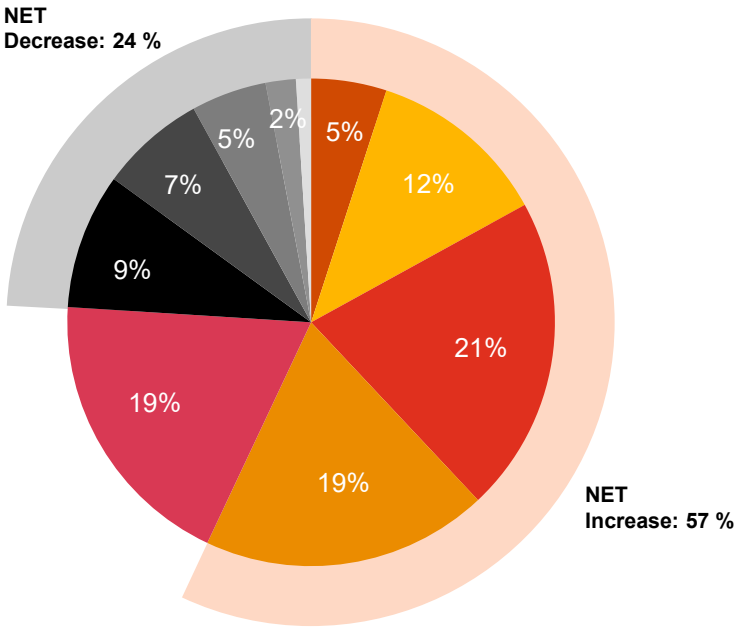
Budget, Investitionen und Kosten durch Angriffe und Datenverluste

Budgets für Security steigen stark – genauso wie die Kosten bei Data Breaches

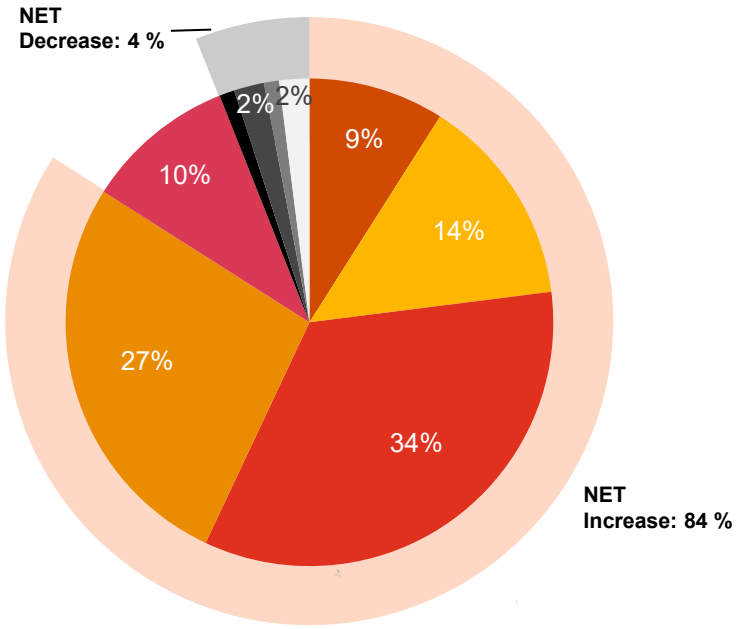
pwc

Steigende Budgets für Cyber Security: 84 % der deutschen Unternehmen wollen mehr ausgeben – nur 4 % kürzen ihr Budget

Veränderung der Cyber-Budgets in 2023



Veränderung der Cyber-Budgets in 2024

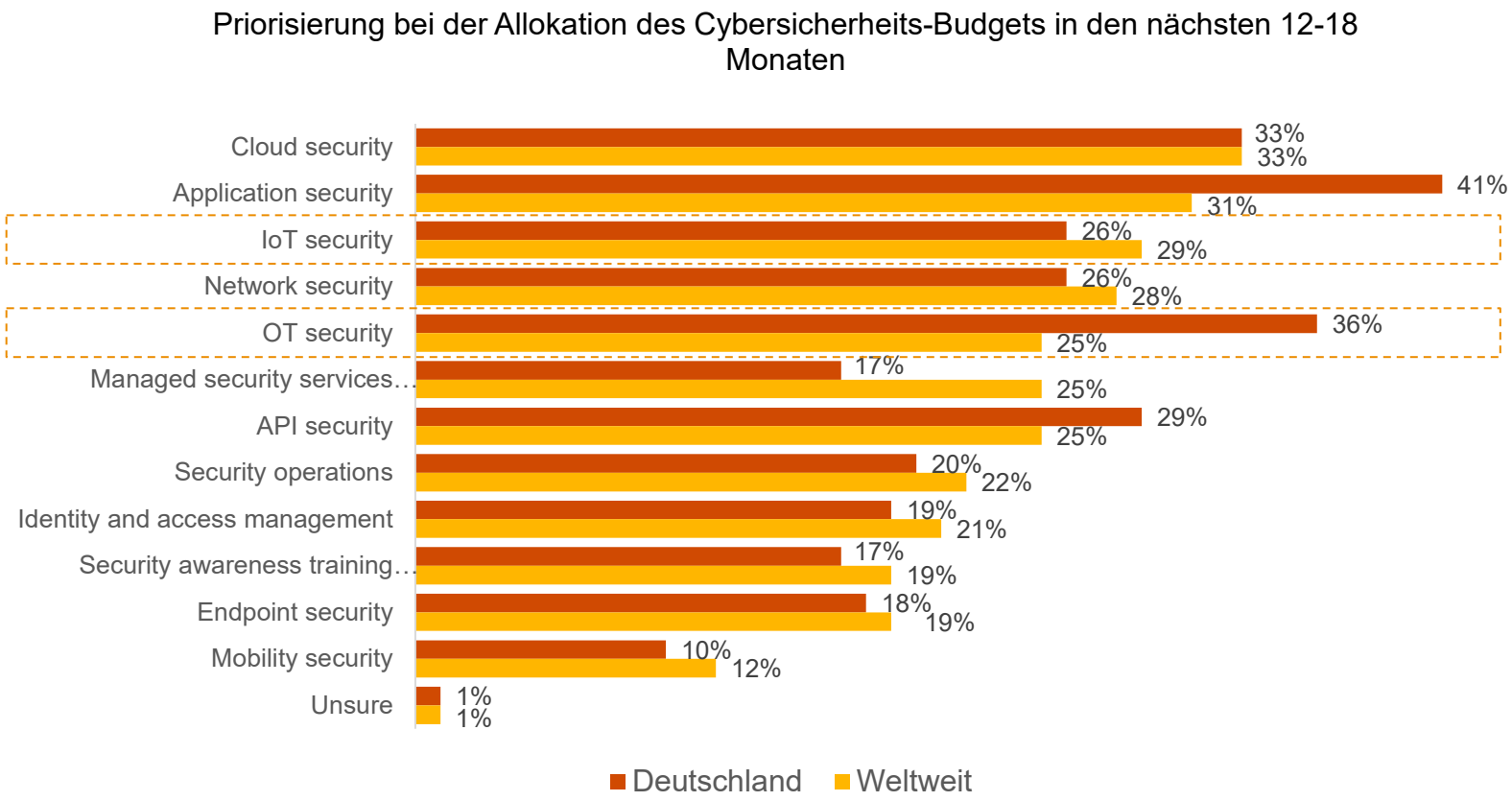


Increase by 15% or more
Increase by 11-14%
Increase by 6-10%
Increase by 5% or less
Unchanged
Decrease by 5% or less
Decrease by 6-10%
Decrease by 11-14%
Decrease by 15% or more
I don't know any detail on the cyber budget
Cannot determine at this time (e.g., due to economic and business uncertainty)

> Die wachsenden Investitionen in die IT-Sicherheit haben neben der raschen Digitalisierung und den neuen Regularien viel mit der geopolitischen Lage zu tun. Zunehmende Spannungen und Bedrohungen im globalen Kontext verdeutlichen, dass digitale Angriffe auch von Staaten und geopolitischen Akteuren ausgehen können. Das erfordert auf Unternehmensseite eine erhöhte Wachsamkeit.
>
> Grant Waterfall, Partner sowie Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

DTI 2023. ALL13a. How is your organisation's cyber budget changing in 2023? Base: Germany=242 | 2024: Q13. How is your organisation's cyber budget changing in 2024? Base: Germany=274
Source: PwC Digital Trust Insights 2024

Während Cloud und IoT Security weltweit im Trend liegen, planen deutsche Führungskräfte verstärkt in Anwendungssicherheit und OT Security zu investieren



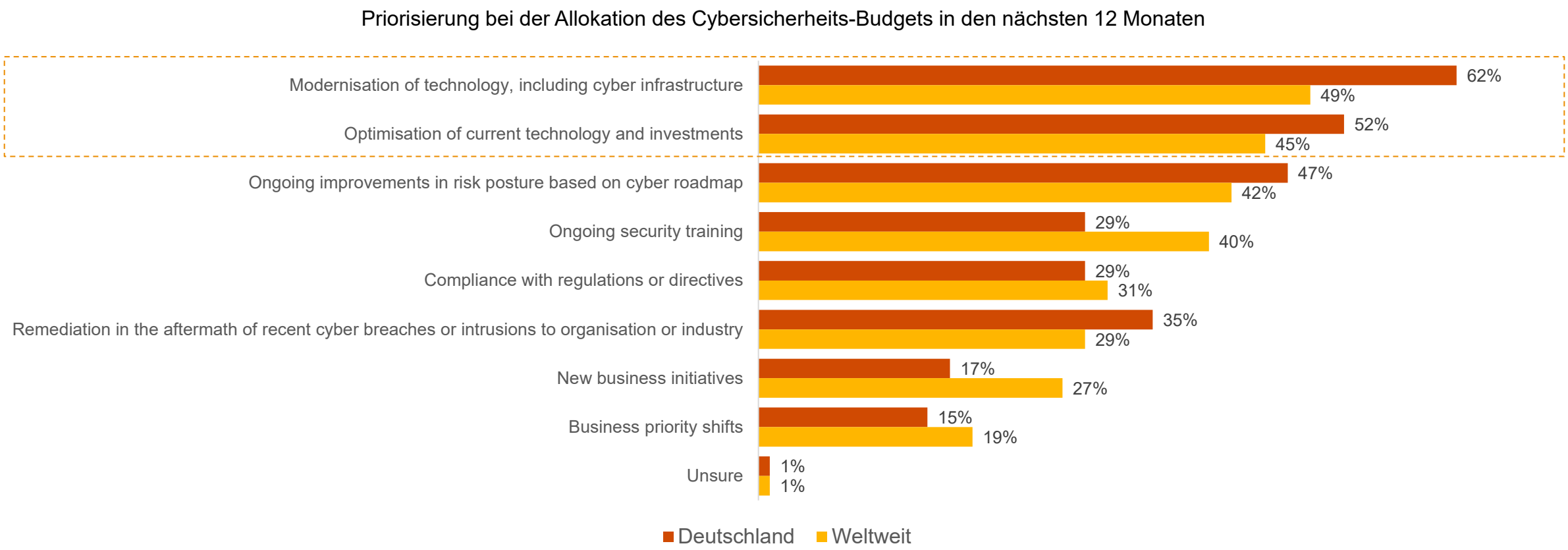
Viele deutsche Industrieunternehmen digitalisieren zunehmend ihre Produktionslandschaft. Um kritische Produktionsprozesse bestmöglich vor Cyberrisiken zu schützen, müssen IT- und OT-Sicherheit optimal integriert und aufeinander abgestimmt werden. Deshalb investieren die Unternehmen verstärkt in diesen Bereich.

Oliver Hanka, Partner, Cyber Security & Privacy bei PwC Deutschland

Q14a. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12-18 months? (Ranked in top three) Base: All respondents=1919 / Germany=170

Source: PwC Digital Trust Insights 2024

Führungskräfte priorisieren Investitionen in die Modernisierung und Optimierung von Technologien – in Deutschland etwas stärker als im Rest der Welt

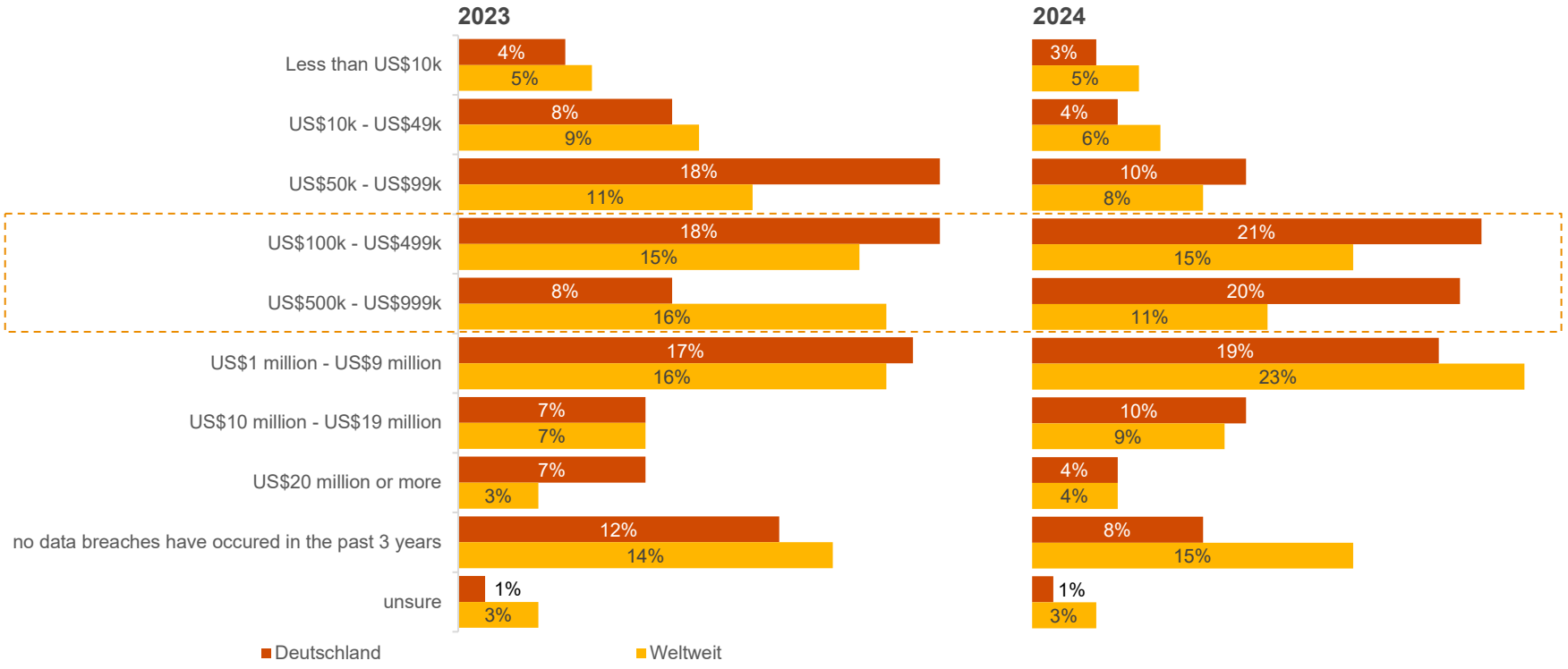


Q14b. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three) Base: All respondents=1925 / Germany=104

Source: PwC Digital Trust Insights 2024

Schäden zwischen 100.000 und 1 Mio. US-Dollar sind stark gestiegen – nur 8 % der Unternehmen aus Deutschland waren die letzten drei Jahre nicht von Datendiebstahl betroffen

Geschätzte Kosten des schadensintensivsten Data Breaches der letzten drei Jahre im Unternehmen



In den letzten drei Jahren sind bei 70 % der befragten Unternehmen in Deutschland Kosten zwischen 100.000 und 20 Millionen US-Dollar entstanden.

Vor allem Schäden im Bereich zwischen 100.000 und 1 Million US-Dollar sind in Deutschland deutlich gestiegen: Berichtete im vergangenen Jahr nur rund ein Viertel der Unternehmen von Kosten in dieser Spanne, sind es jetzt bereits 41 % der Befragten.

2023:
31 % Data Breaches mit $1m+ (global: 26 %)

2024:
33 % Data Breaches mit $1m+ (global: 36 %)

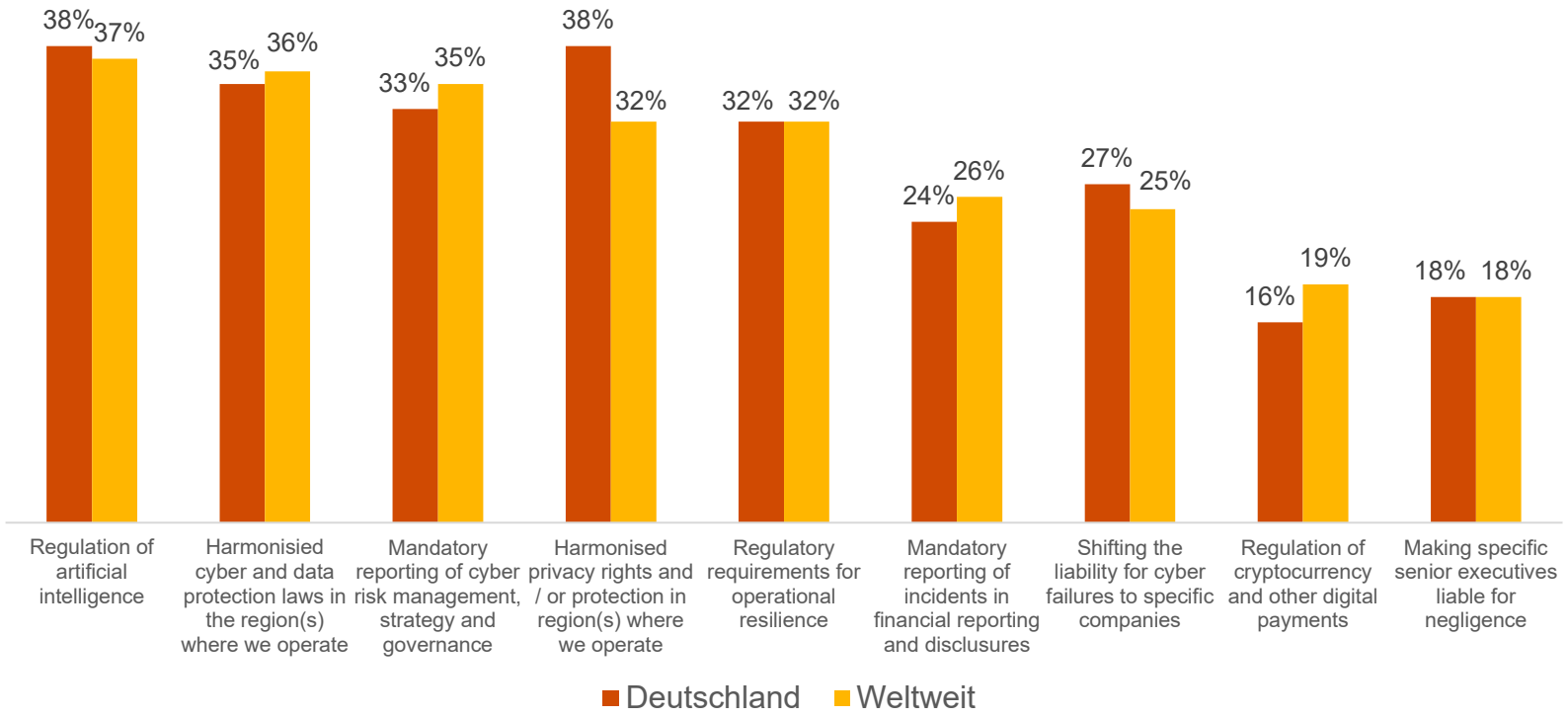
Q5. Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation. Base: Security and IT and CFO respondents= 1651 / Germany= 115
DTI 2023 - CISOTech5 / CFO6: Thinking about the most consequential data breach you experienced in the past three years, please provide an estimate of the cost to your organisation? Base Chief Information Officer (CIO), Chief Technology Officer (CTO), Information Technology Director / VP / Head, CISOs, Chief Security Officers (CSO's), Cybersecurity Director / VP / Head, Information Security Director / VP / Head, CFO, Finance Director / VP / Head (investments)= 1253 / Germany= 76

Regulierung

Unternehmen finden klare Datenschutzgesetze wichtig, rechnen aber mit erhöhten Compliance-Kosten

Deutsche Unternehmen bewerten klare Datenschutzgesetze häufiger als wichtig für das erwartete Umsatzwachstum – die Berichterstattung dagegen seltener

Regulatorische Ziele und Grundsätze mit dem größten Einfluss auf das künftige Umsatzwachstum der Organisation (häufigste Top-3-Nennungen)



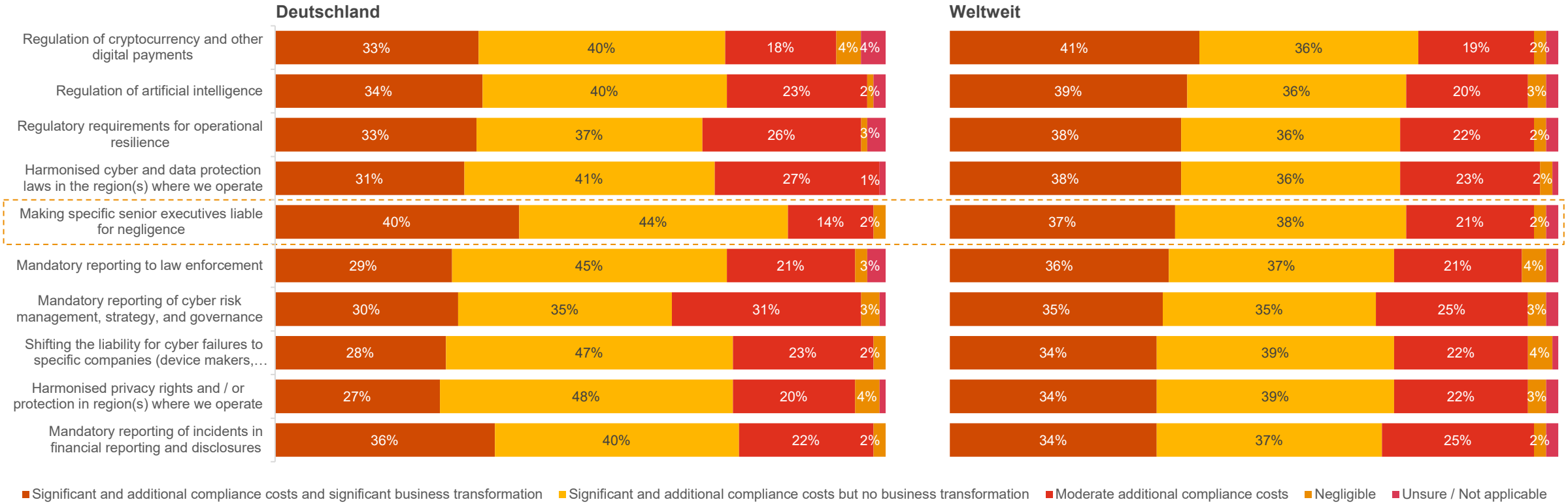
> Viele Unternehmen haben inzwischen verstanden, dass sie in Anbetracht der kommenden Regularien wie NIS-2 oder DORA handeln müssen – nicht nur, um ihre Betriebsabläufe oder Reputation zu schützen, sondern auch aufgrund der hohen finanziellen Folgen bei Verstößen.
>
> André Glenzer, Partner Cyber Security Services bei PwC Deutschland

Q24. Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth? (Ranked in top three) Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

40 % der Unternehmen erwarten in Anbetracht neuer Regularien zu Haftungsfragen signifikant höhere Compliance-Kosten und eine wesentliche Transformation des Geschäfts

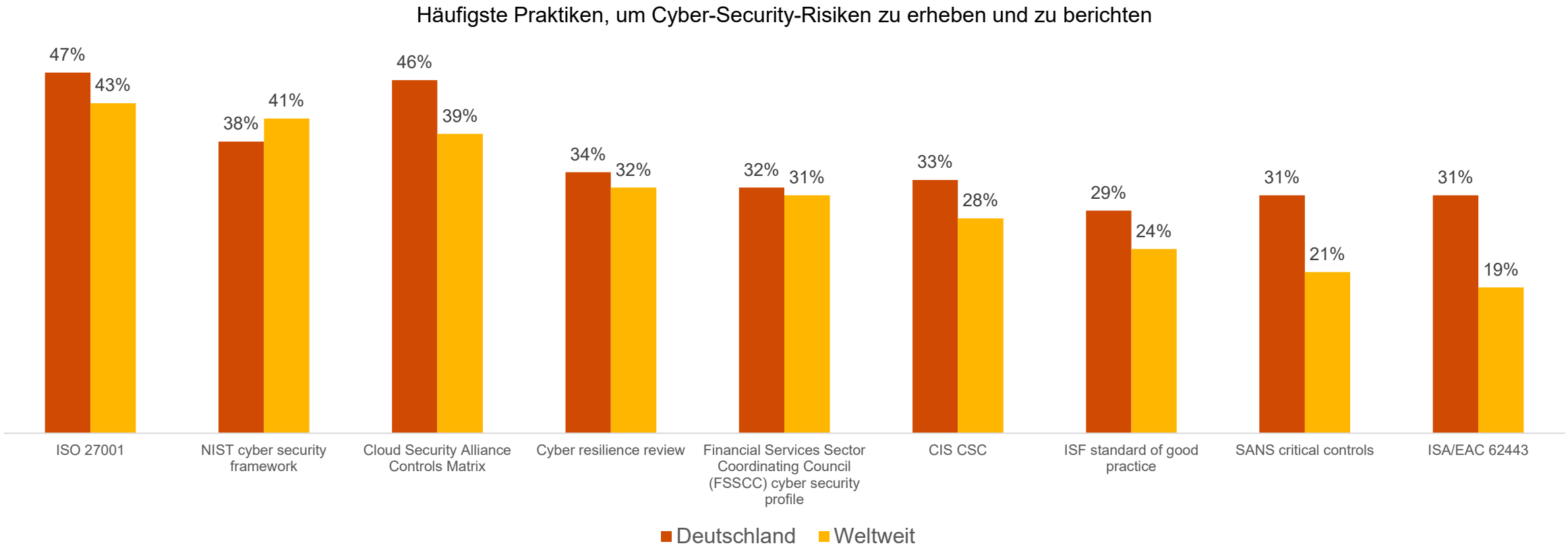
Auswirkungen der regulatorischen Änderungen auf Organisationen



Q19. To what extent has your organisation addressed the following challenges with your cloud service provider(s)? Base: All respondents=3876 / Base: Germany=257

Source: PwC Digital Trust Insights 2024

Für Cybersicherheits-Assessments und Berichte: Gemeinsame Frameworks sind weltweit auf dem Vormarsch, Deutschland ist bei allen bis auf NIST und COBIT Vorreiter bei der Nutzung



Q9. Which of the following does your organisation use to assess and report on your cybersecurity capabilities? Base: Security and IT respondents=1517 / Germany=110

Source: PwC Digital Trust Insights 2024

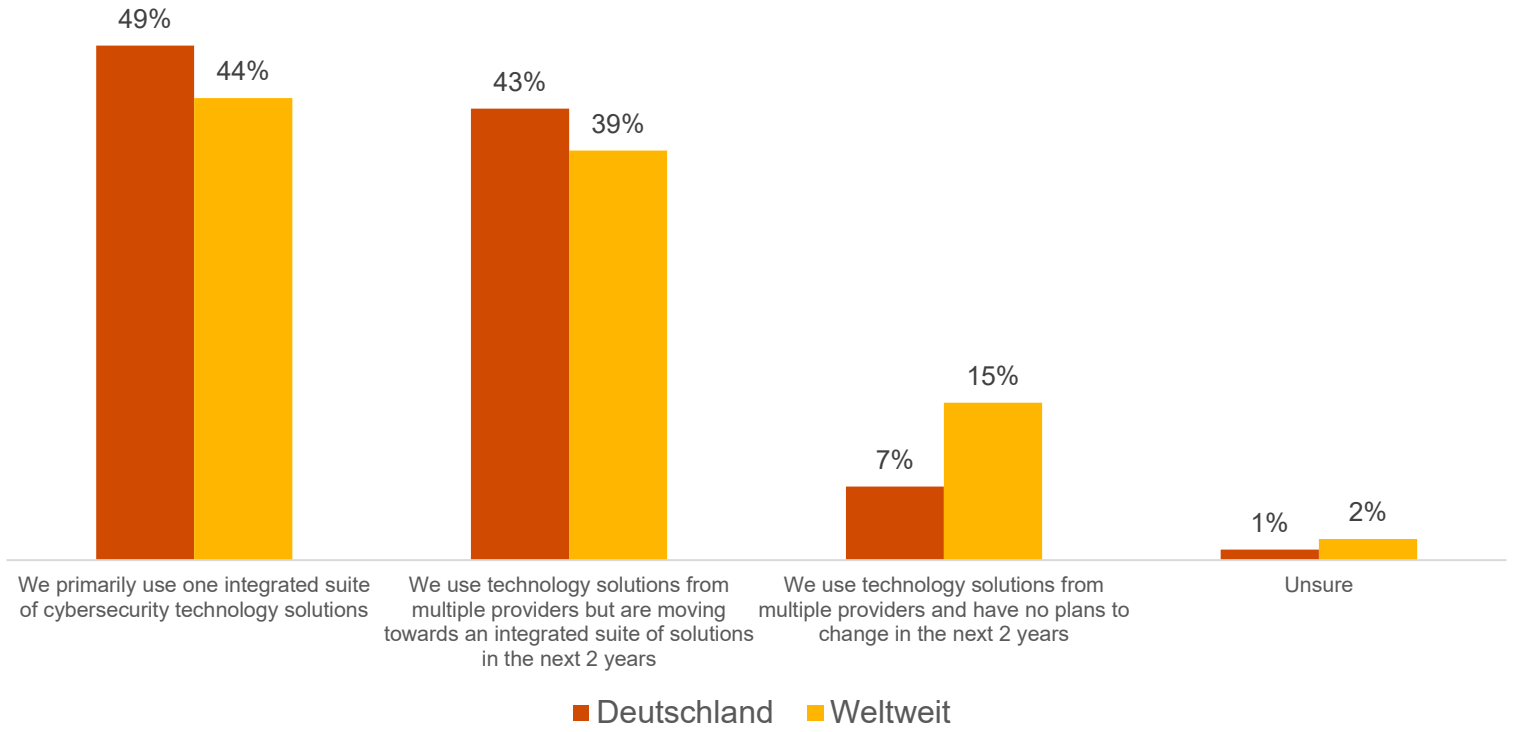
Integrierte Cyber-Technologie-Plattformen

Knapp die Hälfte der deutschen Befragten nutzt bereits integrierte Cyber-Technologie-Plattformen

pwc

2 von 5 Unternehmen wollen in den nächsten 12 Monaten zu integrierten Cyber-Technologie-Lösungen wechseln

Unterschiedliche Herangehensweisen an Cybersecurity-Technologien



Q20. Which of the following best describes your organisation's current approach to cybersecurity technology? Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

> Der Trend ist klar: In Kürze werden 9 von 10 Unternehmen in Deutschland mit integrierten Cyber-Technologie-Plattformen arbeiten. Diese bieten gegenüber herkömmlichen Lösungen viele Vorteile. Sie reduzieren die Komplexität, erhöhen die Reaktionszeit und vereinfachen die Durchsetzung von Richtlinien.
>
> Grant Waterfall, Partner sowie Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

Nur jedes 20. deutsche Unternehmen gibt an, zu wenig Einzellösungen zu nutzen, fast jedes Zehnte würde dagegen weiter reduzieren

Q22. Which of the following statements do you agree with most? Base: Security and IT respondents=1517 / Germany=110

Source: PwC Digital Trust Insights 2024

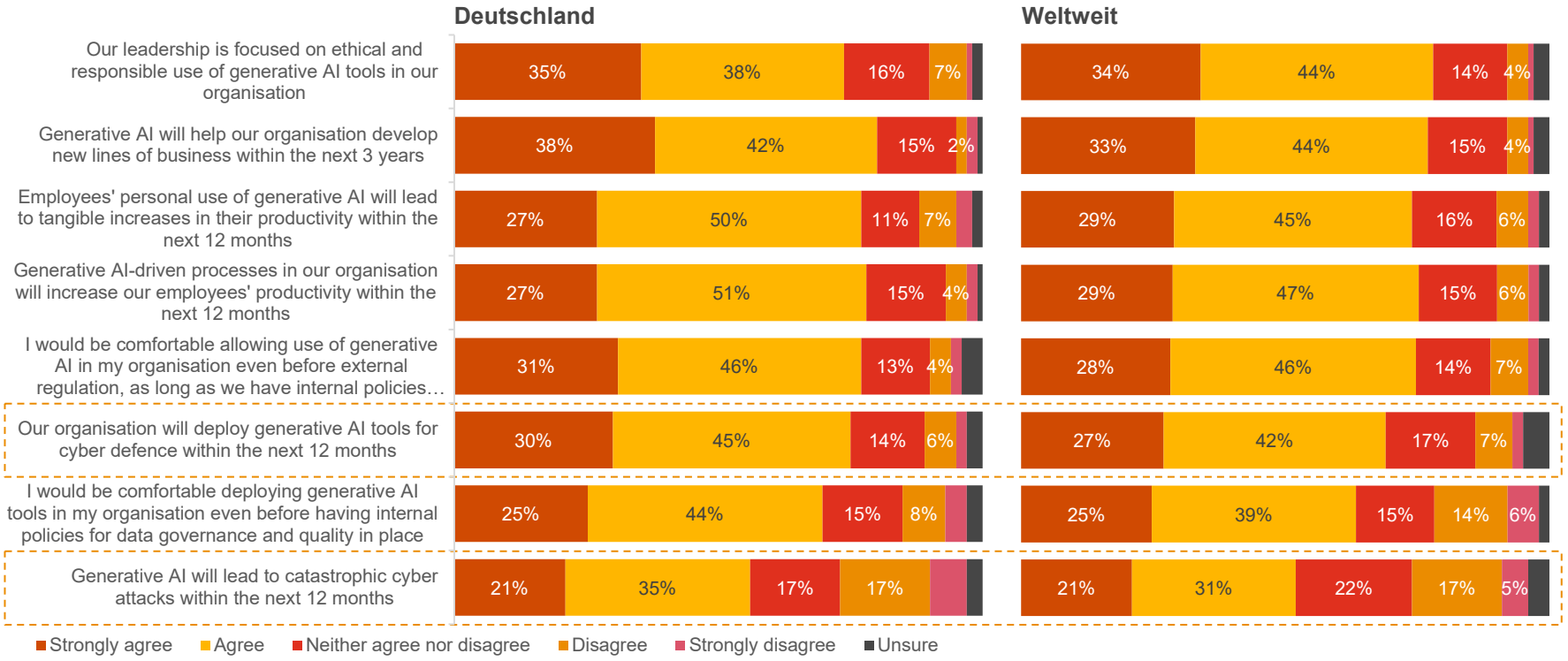
DefenceGPT: Generative KI in der Cyber Security

Relevanz von Generativer KI nimmt zu – sowohl auf Seiten der Angreifer als auch der Security

pwc

7 von 10 Unternehmen wollen im nächsten Jahr auf generative KI zur Cyberabwehr setzen – die Hälfte rechnet mit verheerenden KI-getriebenen Angriffen

Haltung zur generativen KI des Unternehmens



Q7. To what extent do you agree or disagree with the following statements about Generative AI? Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

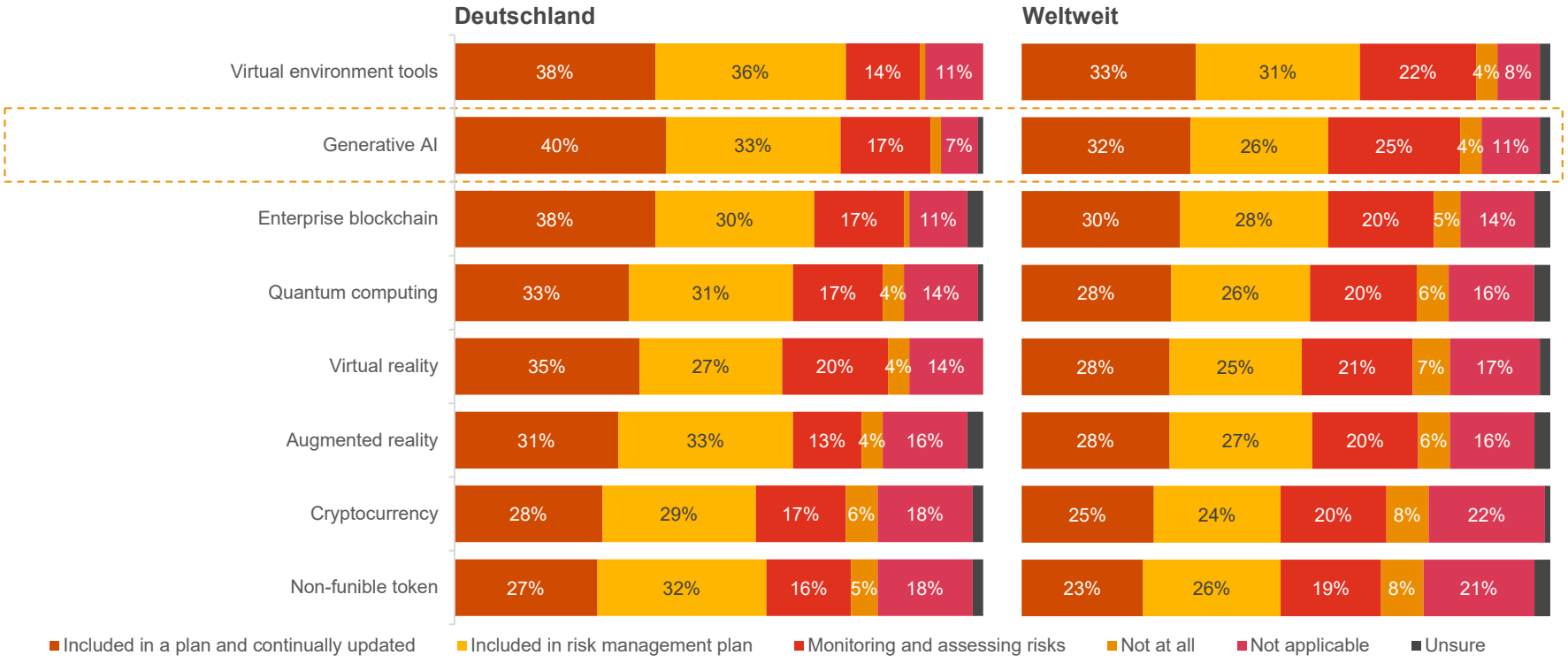
Volle Zustimmung für GenAI:

- **35 %** sagen, dass ihre **Führung sich auf den ethischen und verantwortungsvollen Einsatz von generativen KI-Tools in ihrem Unternehmen konzentriert** (global: 34 %).
- **38 % wird** GenAI in den nächsten 3 Jahren helfen, **neue Geschäftsfelder** zu entwickeln (global: 33 %).
- **75 %** werden innerhalb der nächsten 12 Monate **GenAI-Tools für die Cyberabwehr** einsetzen (global: 69 %).

> Viele Unternehmen haben das Potenzial von GenAI im Bereich Cyber Defence erkannt. Dass sowohl in Deutschland als auch global nur die Hälfte der Befragten mit verheerenden Cyberangriffen auf Basis von generativer KI rechnet, verdeutlicht aber, dass vielen die Gefahren der Technologie noch nicht gänzlich bewusst sind. Hier braucht es definitiv noch mehr Aufklärungsarbeit.
>
> Hendrik Reese, Partner und Experte für Trust in AI bei PwC Deutschland

3 von 4 deutschen Unternehmen berücksichtigen GenAI in ihrer Risikomanagementplanung, davon gut die Hälfte in fortlaufend aktualisierten Plänen

Verständnis der Organisation für Cyberrisiken im Zusammenhang mit neuen Technologien



Über alle Technologien hinweg, werden bei mehr als 25 % die Cyberrisiken nicht in einen Risikomanagementplan aufgenommen. Global sind es durchschnittlich sogar mehr als 40 %.

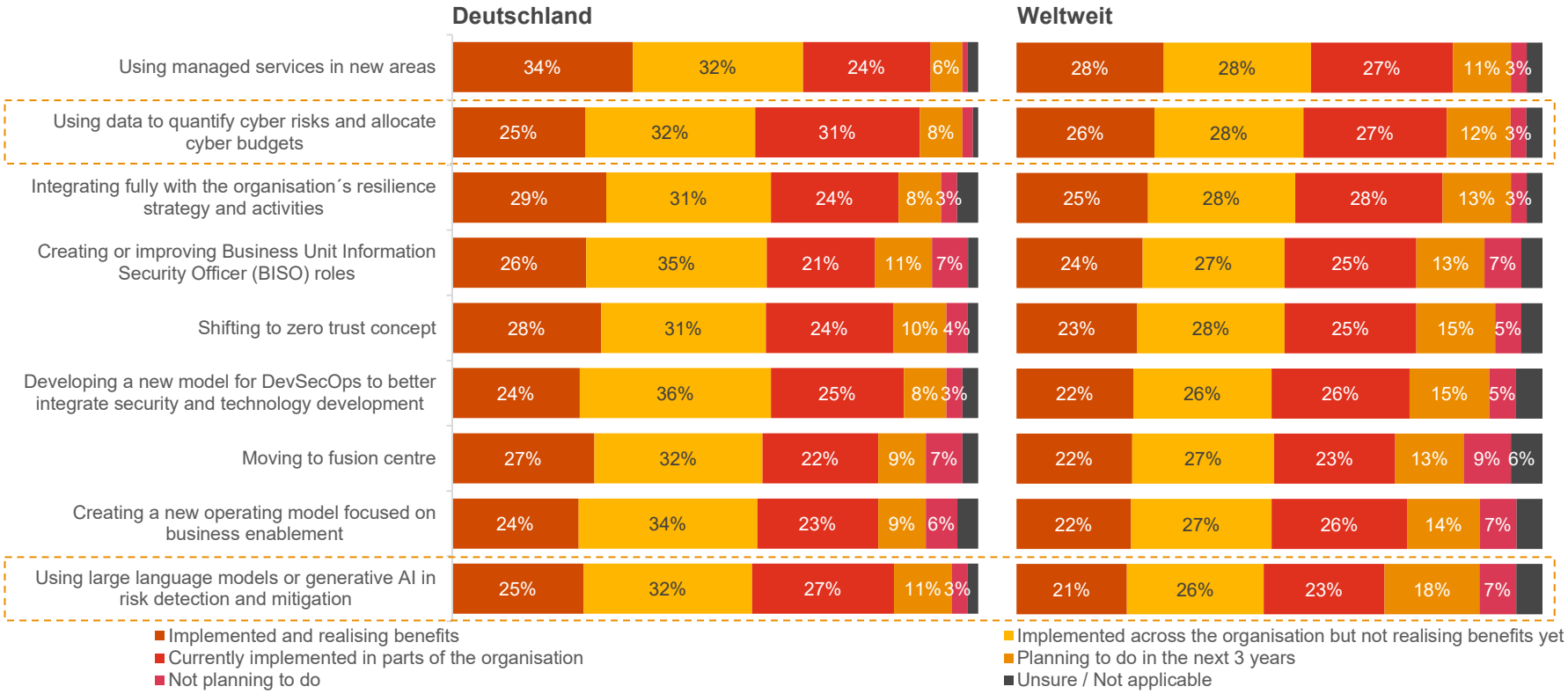
Deutsche Unternehmen verfügen häufiger über einen kontinuierlichen Implementierungsplan für **GenAI** als Unternehmen weltweit (40 vs. 32 %).

Q6. To what extent does your organisation understand the cyber risks related to the following technologies? Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

Zwei Drittel der deutschen Unternehmen setzen bereits auf Managed Services als Maßnahme für mehr Cybersicherheit; Deutschland ist besonders bei GenAI Vorreiter

Implementierungsgrad von Cyber-Security-Initiativen in Organisationen



Weltweit hat erst knapp die Hälfte der Organisationen **generative KI oder LLM** für die Risikoerkennung und -minderung innerhalb der gesamten Organisation implementiert, in **Deutschland sind es bereits 6 von 10** (57 vs. **47 %**).

Zudem nutzen deutsche Unternehmen bereits häufiger Daten, um Cyberrisiken zu quantifizieren und Budgets zu allokieren. (88 vs. 81 %)

Q10. To what extent is your organisation implementing or planning to implement the following cybersecurity initiatives? Base: All respondents=3876 / Germany=274

Source: PwC Digital Trust Insights 2024

Methodik und Stichprobe

Global Digital Trust Insights 2024: Die älteste und umfangreichste Umfrage ihrer Art

3.876

Führungskräfte aus den Bereichen Business, Technologie und Sicherheit inklusive CEOs, Vorstand, CFOs, CISOs, CIOs, CTOs – 274 davon aus Deutschland

71 Länder

W. Europe (32 %), N. America (28 %), Asia Pacific (18 %), Latin America (10 %), E. Europe (5 %), Africa (4 %), Mid-East (3 %)

67 %

Unternehmen mit einem Umsatz von 1 Mrd. US-Dollar oder mehr

26. Ausgabe

des globalen Cyber Security Reports von PwC

Hier geht's zum globalen Report: www.pwc.com/dti2024

Deep Dive Read: Nutzung von Generativer KI für Cyber Security

Hier geht's zur Always-on-Befragung. Jetzt teilnehmen und Benchmark-Bericht für das eigene Unternehmen erhalten!

Source: PwC Digital Trust Insights 2024

Über die Umfrage

PwC hat die „Digital Trust Insights“-Studie entwickelt, um von Führungskräften zu erfahren, welche Chancen und Herausforderungen sie innerhalb der nächsten 12 bis 18 Monate in Hinblick auf die Cybersicherheit in ihren Unternehmen erwarten. Die Kernfragen sind so konzipiert, dass sie von Befragten aller Berufsgruppen beantwortet werden können. Ein zusätzlicher Satz von Fragen wurde denjenigen gestellt, die im Bereich Sicherheit und IT tätig sind (CIO, CSO, CTO, Direktor für Cybersicherheit, Direktor für Informationssicherheit, Direktor für Informationstechnologie).

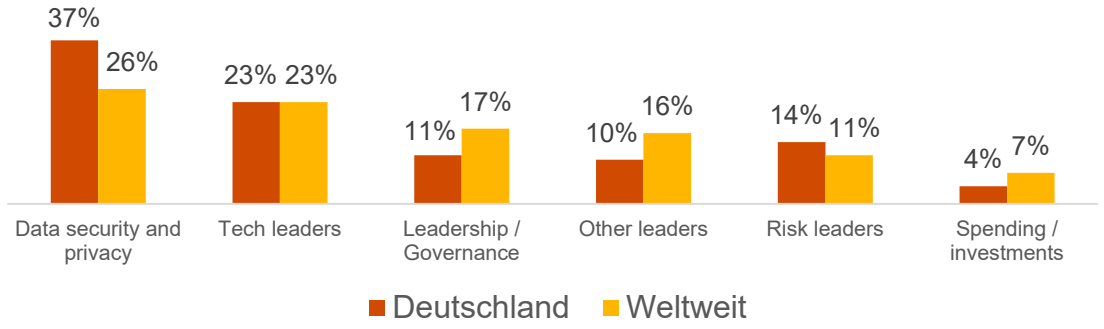
Die Ergebnisse basieren auf Antworten von 3.876 Befragten aus 71 Ländern. 274 der Befragten kommen aus Deutschland. Die Teilnehmenden stammen aus verschiedenen Branchen (industrielle Fertigung, Technologie, Medien, Telekommunikation, Finanzdienstleistungen, Handel, Konsumgüter, Energieversorger, Rohstoffwirtschaft, Gesundheitswesen, Regierung, Öffentlicher Dienst) und Unternehmensgrößen. 40 % der Unternehmen haben einen Umsatz von mehr als 5 Mrd. US-Dollar.

Aufgrund von Rundungen kann es vorkommen, dass sich die Prozentzahlen nicht auf 100 % addieren.

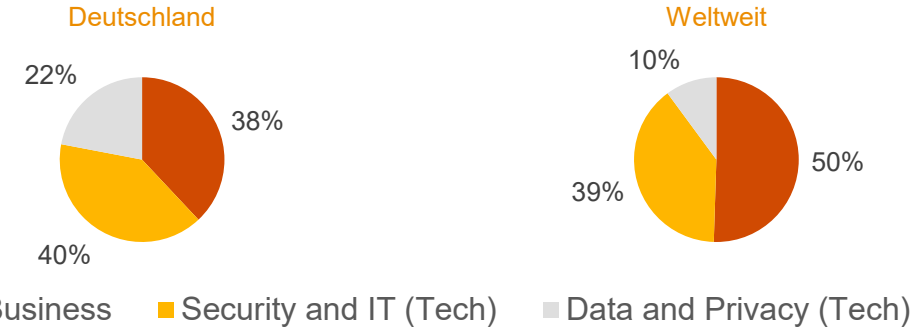
Source: PwC Digital Trust Insights 2024

274 deutsche Befragte aus allen Branchen – 62 % haben Tech-Hintergrund und 30 % kommt aus Unternehmen mit Umsatz >10 Mrd. US-Dollar

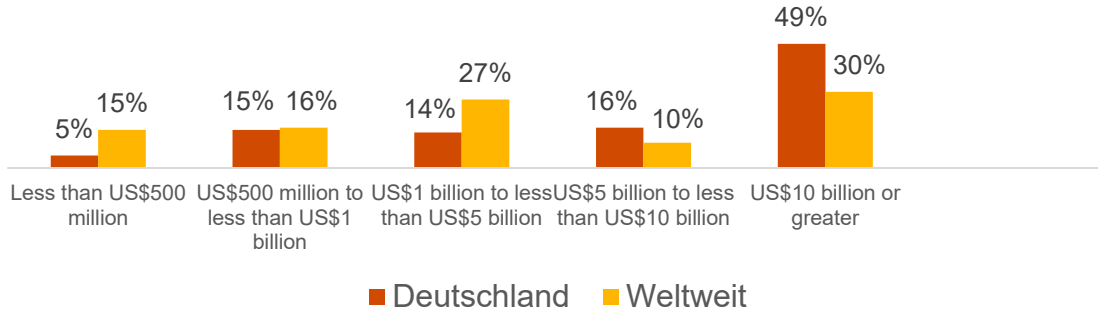
Jobtitel



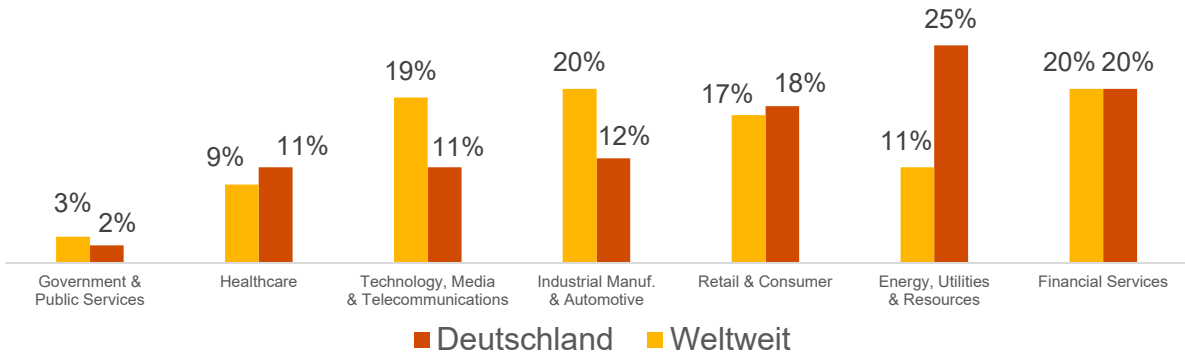
Jobtitel: Klassifikation der Jobprofile der Befragten



Umsatz



Branchen



Total = 3876; Germany = 274

Source: PwC Digital Trust Insights 2024

pwc.de