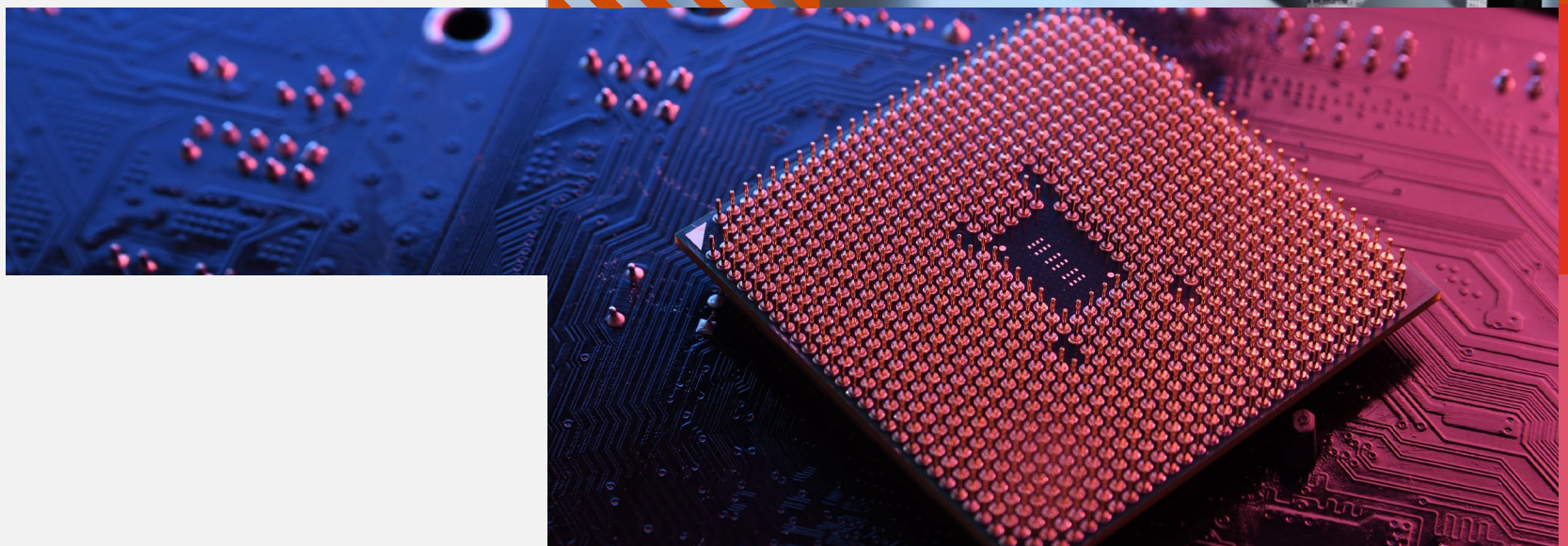
Global Digital Trust Insights 2025

Studienergebnisse für Deutschland
Oktober 2024



Management Summary für die C-Suite
Cyberresilienz mit Lücken – hier sollten Sie am Ball bleiben

Neue Herausforderungen werden Normalität

- Technologiesprünge und Transformationsinitiativen verändern die Vorzeichen für Cybersicherheit. Sie schaffen **neue Angriffsflächen** und **erhöhen die Komplexität** der Abwehrmaßnahmen.
- Die Prioritäten der Risikominderung haben sich im Vergleich zum Vorjahr verschoben: **Cyberrisiken haben nun mit 56 % die höchste Relevanz,** knapp gefolgt von digitalen und technologischen Risiken (50 %).

Deutsche Unternehmen häufiger betroffen

- Deutsche Unternehmen waren in den letzten drei Jahren **häufiger Opfer von Datendiebstahl und -missbrauch** (Data Breaches) als Unternehmen weltweit. 83 % kostete ein Data Breach bis zu 9,9 Mio. US-Dollar, 8 % berichten von Schäden zwischen zehn und 20 Mio. Dollar oder mehr.

Lücken müssen geschlossen werden

- Viele Unternehmen haben Cyberresilienzmaßnahmen zum Teil implementiert. Allerdings gibt es eklatante Lücken bei der **vollständigen unternehmensweiten Umsetzung.** Die Abbildung von Technologieabhängigkeiten, die Einrichtung eines Resilienz-Teams oder eine Simulation von Gefahren haben jeweils weniger als ein Drittel der Unternehmen in Deutschland implementiert – Cyber-Wiederherstellungsmaßnahmen wiederum haben zumindest 47 % vollständig umgesetzt.
- Trotz dieser Lücken zeigt die Studie, dass sich Unternehmen der Gefahren bewusst sind und handeln: **72 %** der deutschen Unternehmen planen, ihr **Budget für Cyberresilienz zu erhöhen.**

Digital Trust Insights 2025 – Deutschland
6 Kernthemen

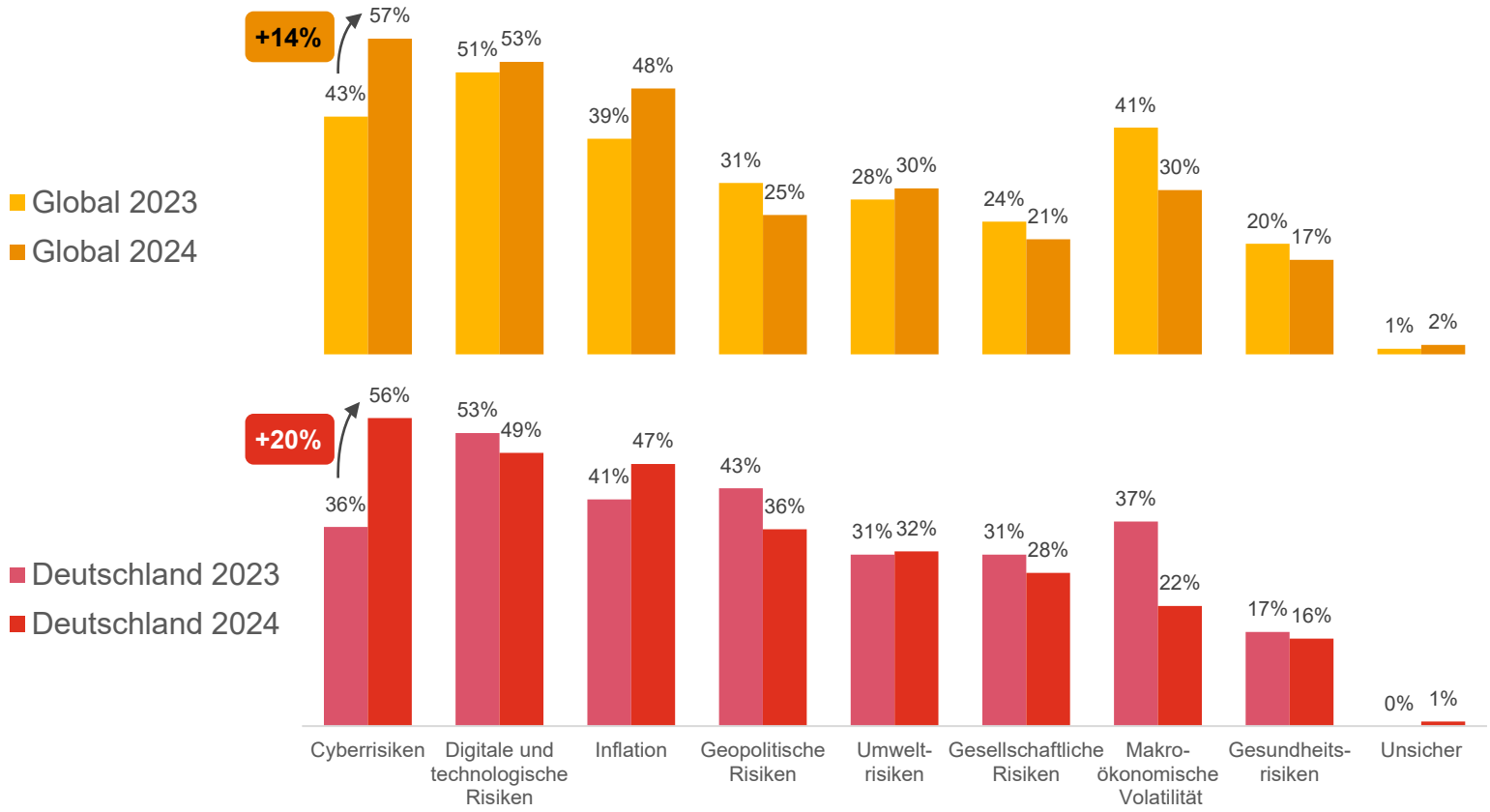
1

Risiken und Bedrohungs-szenarien

Cyberrisiken in den Griff bekommen wird höchste Priorität

Die Prioritäten der Risikominderung haben sich im Vergleich zum Vorjahr deutlich verschoben: **Cyberrisiken haben nun die höchste Relevanz** (+20%), knapp gefolgt von digitalen und technologischen Risiken und Inflation. Die Verschiebung spiegelt die zunehmende Abhängigkeit von Technologien und den damit verbundenen potenziellen Gefahren wider.

Cyberrisiken stehen ganz oben auf die Agenda der Risikominderung



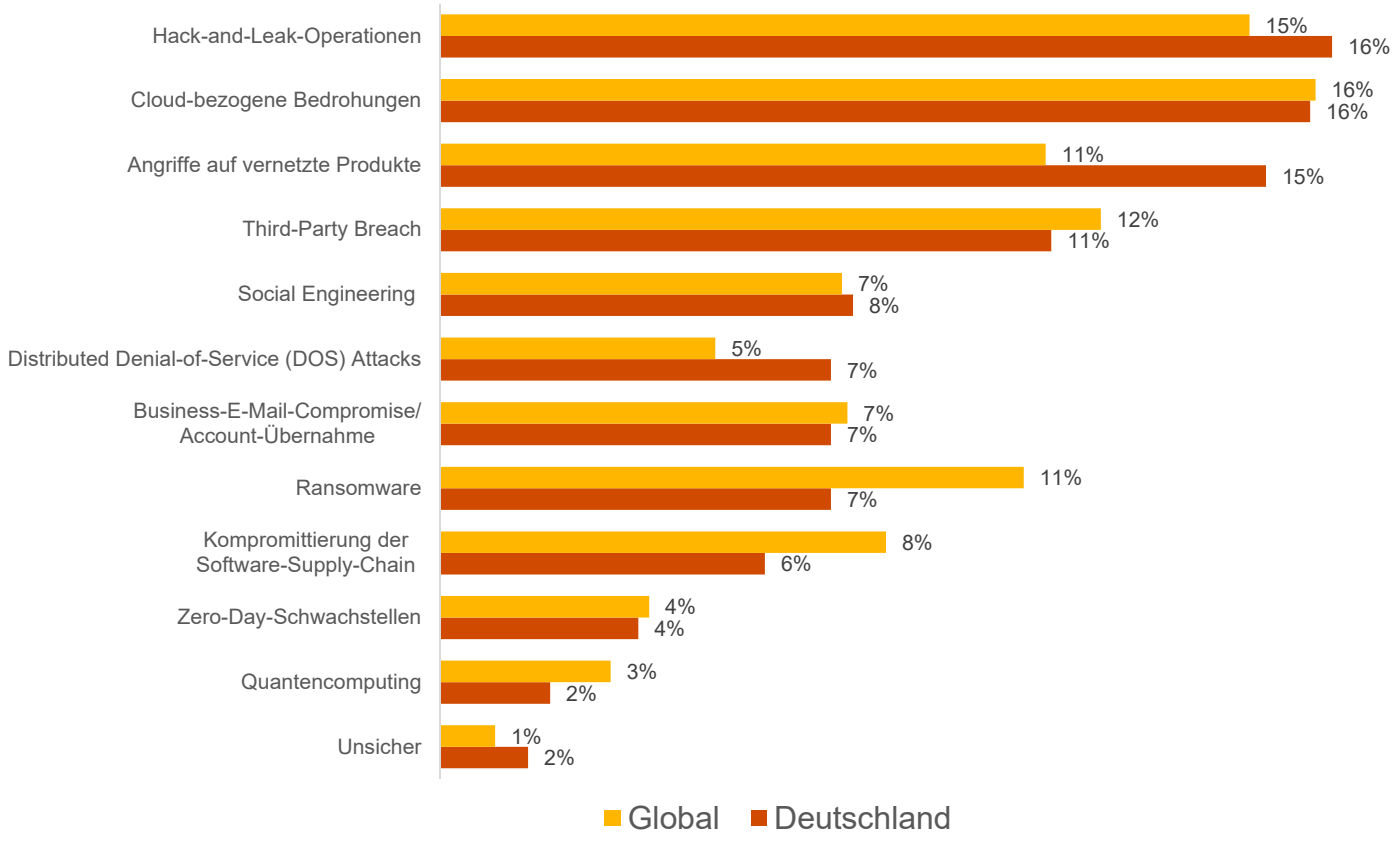
Fragestellung: Welchen der folgenden Risiken wird Ihre Organisation in den nächsten 12 Monaten vorrangig entgegenwirken? Kumulierte Nennung der Top 3. Basis: Alle Unternehmen (2025: 4042 Global / 253 Deutschland; 2024: 3876 Global / 274 Deutschland)

Sorge um Kompromittierung von Cloud und Daten

Die Gefährdung von digitalen Infrastrukturen bereitet weltweit den meisten Befragten Sorgen. In Deutschland dominiert die Angst vor **Hack-and-Leak-Operationen**, gefolgt von Cloud-bezogenen Bedrohungen und Angriffen auf vernetzte Produkte.

> Die sichere Integration und Verwaltung von Cloud-Technologien erfordert spezialisierte Fachkenntnisse, die oft fehlen – und die in Anbetracht des weit verbreiteten IT-Fachkräftemangels auch nur schwer zu bekommen sind.
>
> Grant Waterfall, Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

Von diesen Cybervorfällen fühlen sich Unternehmen am stärksten bedroht

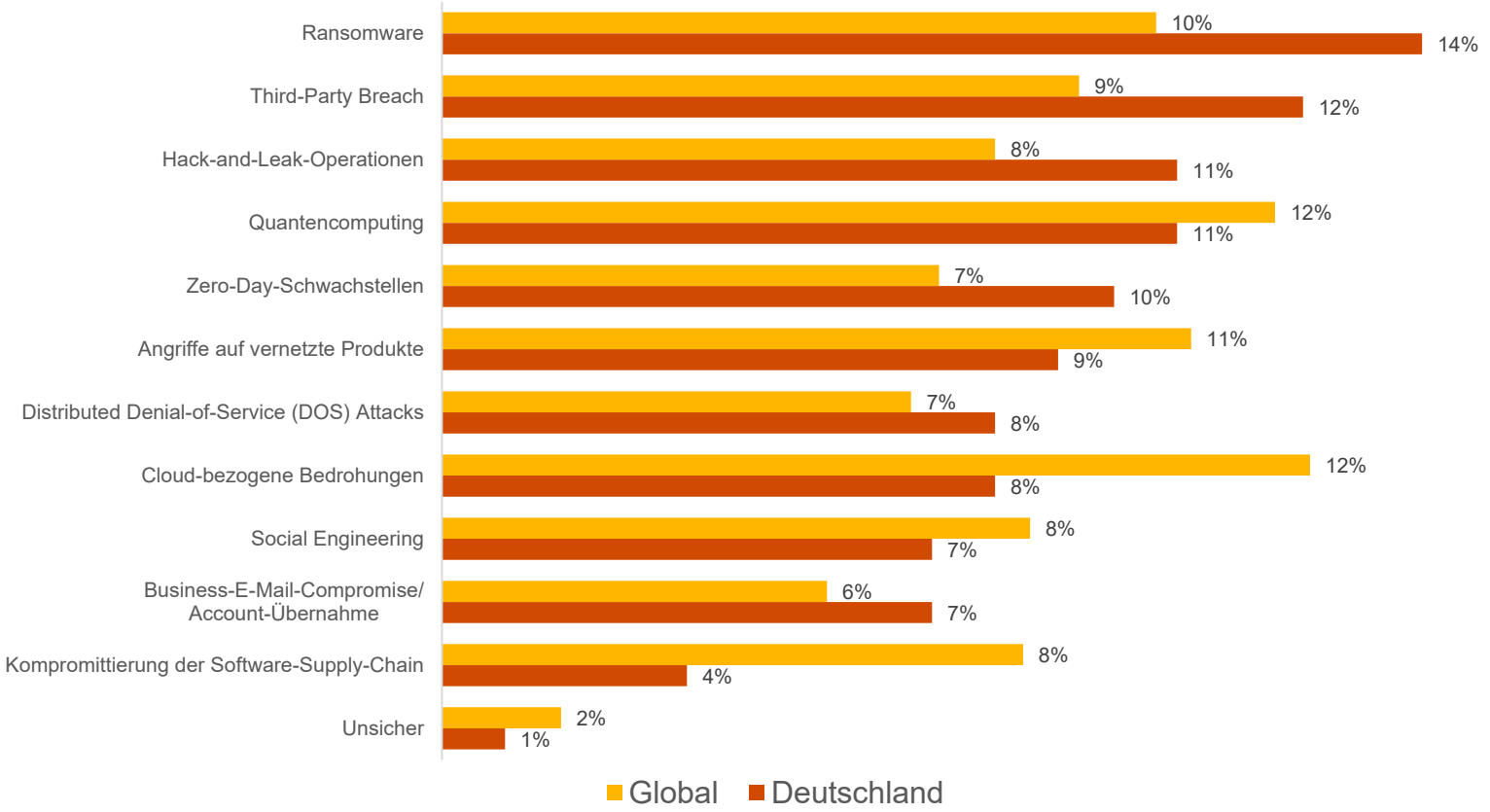


Fragestellung: Über welche der folgenden Cyberbedrohungen macht sich Ihr Unternehmen in den nächsten 12 Monaten am meisten Sorgen? Basis: Alle Unternehmen (4042 Global / 253 Deutschland)

Unzureichende Vorbereitung auf viele Cybergefahren

In Deutschland fühlen sich mehr Unternehmen zu wenig für komplexe Bedrohungen wie **Ransomware oder Third-Party Breaches** gewappnet als weltweit; die Einschätzungen für andere Angriffsformen weichen zum Teil ab. Aber: Die Bedrohungslage von unterschiedlichen Seiten wird klar erkannt.

Bei diesen Cyberbedrohungen gibt es Nachholbedarf in Sachen Cyberabwehr und Resilienz



Fragestellung: Auf welche der Cyberbedrohungen ist Ihr Unternehmen Ihrer Meinung nach in den nächsten 12 Monaten am wenigsten vorbereitet? Basis: Befragte aus den Bereichen Sicherheit und CFOs (1951 Global / 114 Deutschland)

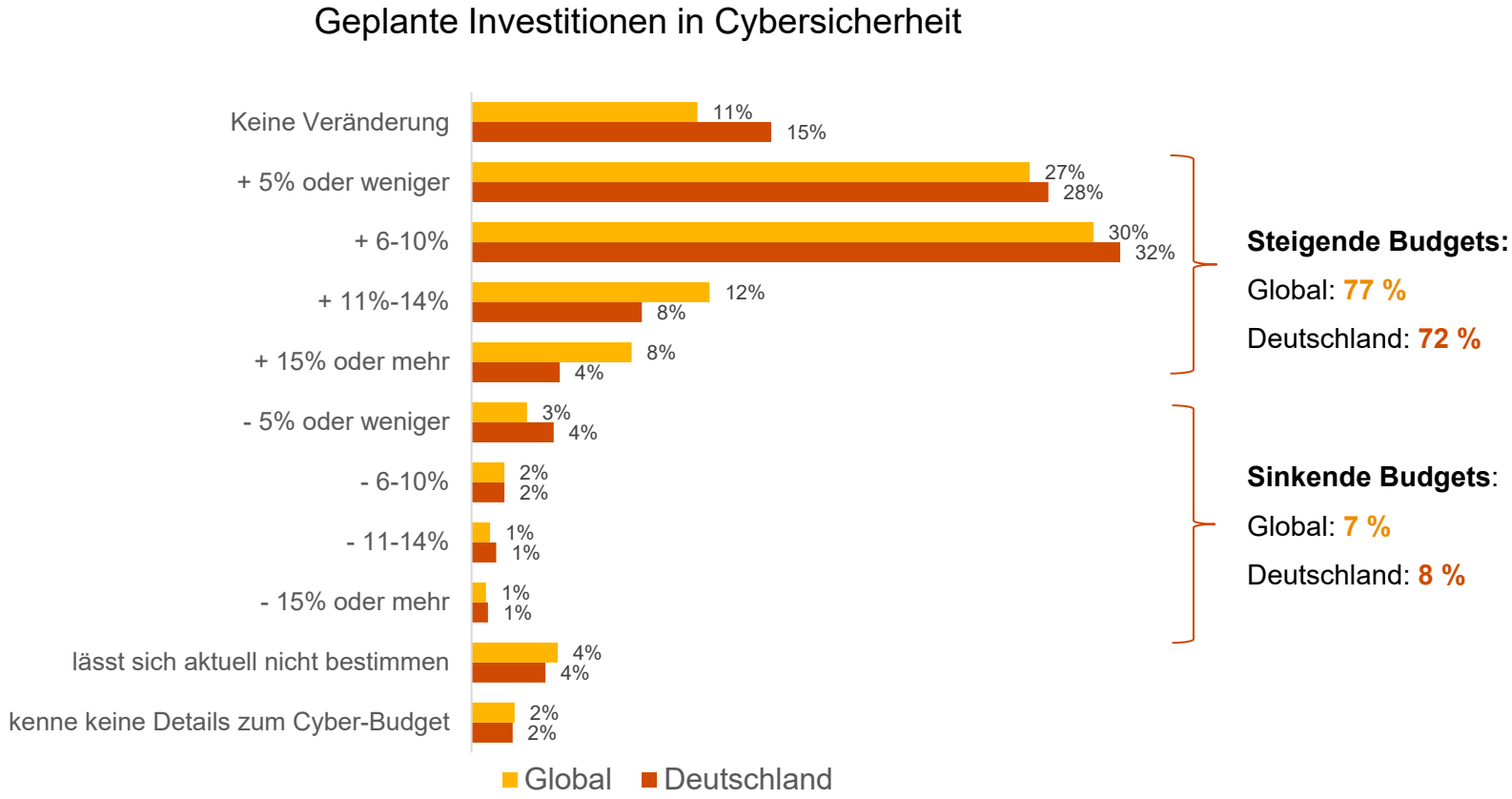
2

Budgets und Investitionen

Hoher Stellenwert von Cybersicherheit sorgt für stabile Budgets

Die Budgets für Cybersicherheit und Resilienz bleiben stabil – mit einem leichten Aufwärtstrend. 15 % der Investitionen bleiben ähnlich hoch wie im Vorjahr, wobei kleinere Unternehmen weiterhin einen höheren Prozentsatz investieren als größere Unternehmen.

In Zukunft soll mehr investiert werden: 72 % der befragten deutschen Unternehmen planen, ihr Budget zu erhöhen.



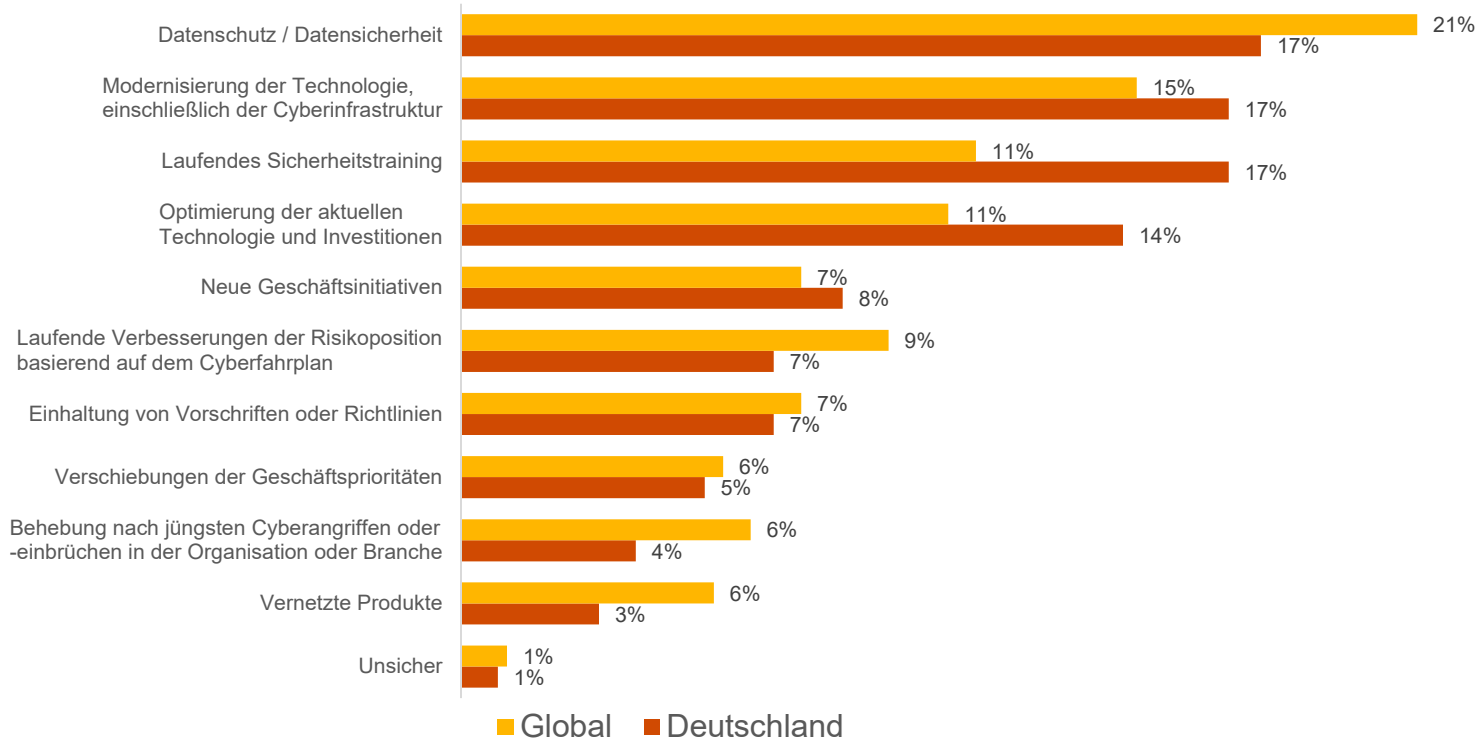
Fragestellung: Wie wird sich das Cyberbudget Ihrer Organisation im Jahr 2025 verändern? Basis: Alle Unternehmen (4042 Global / 253 Deutschland)

Unternehmen investieren verstärkt in Datenschutz

Die befragten Verantwortlichen priorisieren wie bereits im letzten Jahr vor allem Datenschutz und Technologiemodernisierung – inklusive der Cyberinfrastruktur – bei ihren Investitionen.

> In den kommenden Jahren müssen Unternehmen ihre Cyberstrategien und -investitionen proaktiv anpassen, um den steigenden Herausforderungen durch neue Technologien und wachsende Regulierung gerecht zu werden.
>
> Grant Waterfall, Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

Regulatorik und Modernisierungsdruck beeinflussen Investitionen in Cybersicherheit

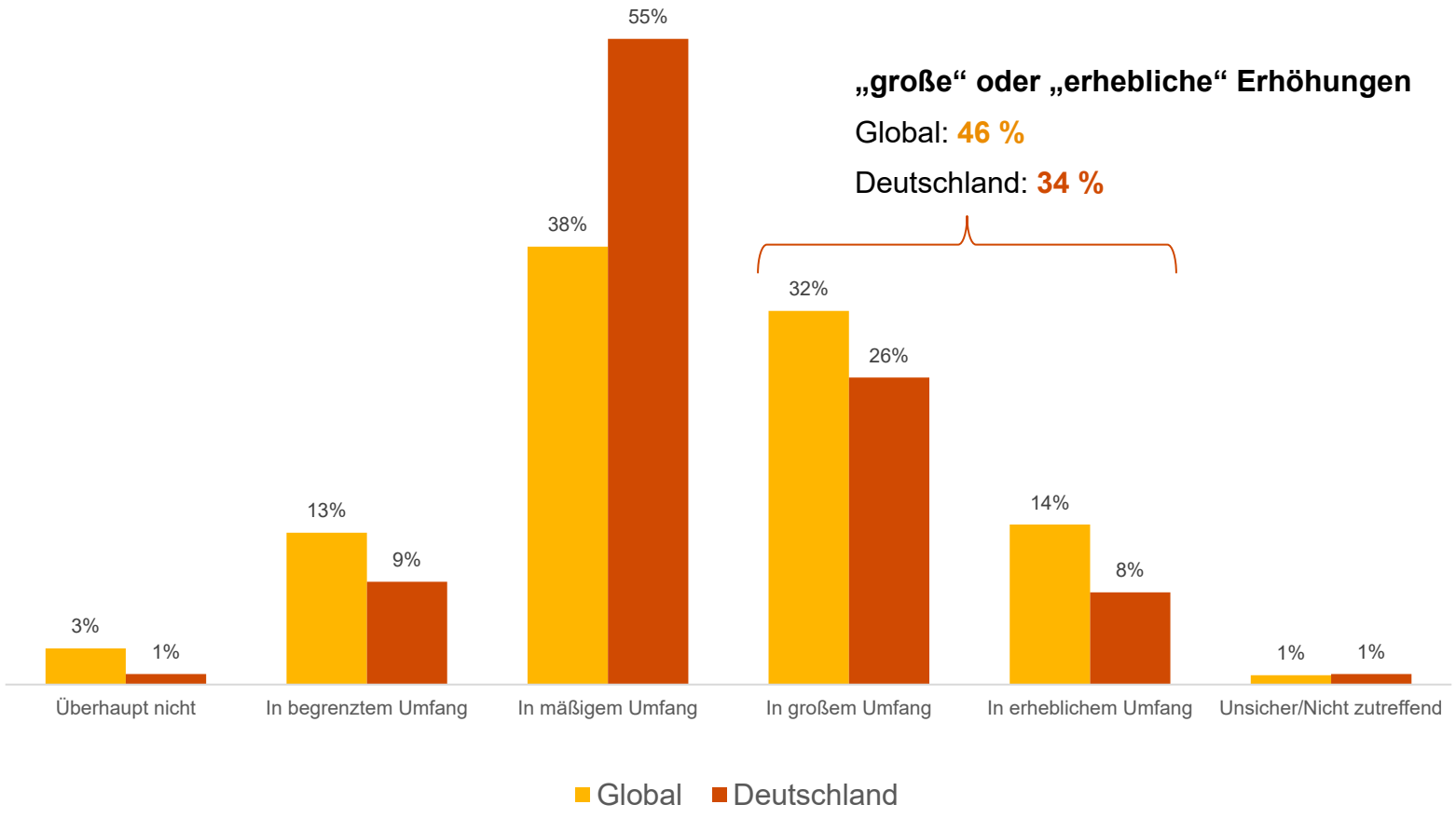


Fragestellung: Welche der folgenden Investitionen haben für Sie bei der Zuweisung des Cyberbudgets Ihrer Organisation in den nächsten 12 Monaten Priorität? Basis: Alle befragten Unternehmen mit Kenntnis der Veränderungen im Cyberbudget (1876 Global / 132 Deutschland)

Regulierung treibt Investitionen in die Höhe

Fast alle befragten Unternehmen haben festgestellt, dass sich die gesetzlichen Vorschriften zur Cybersicherheit auf ihre Investitionen in den letzten 12 Monaten ausgewirkt haben, wobei in Deutschland etwas mehr als die Hälfte der befragten Unternehmen (55 %) mäßige und rund ein Drittel große oder erhebliche Folgen festgestellt hat.

Erhöhung von Budgets für die Erfüllung von NIS-2, DORA, Cyber Resilience Act & Co.



Fragestellung: Inwieweit, wenn überhaupt, haben die Cybersicherheitsvorschriften in den letzten 12 Monaten die Investitionen Ihres Unternehmens in die Cybersicherheit erhöht? Basis: Befragte aus den Bereichen Sicherheit und CFOs (1951 Global / 114 Deutschland)

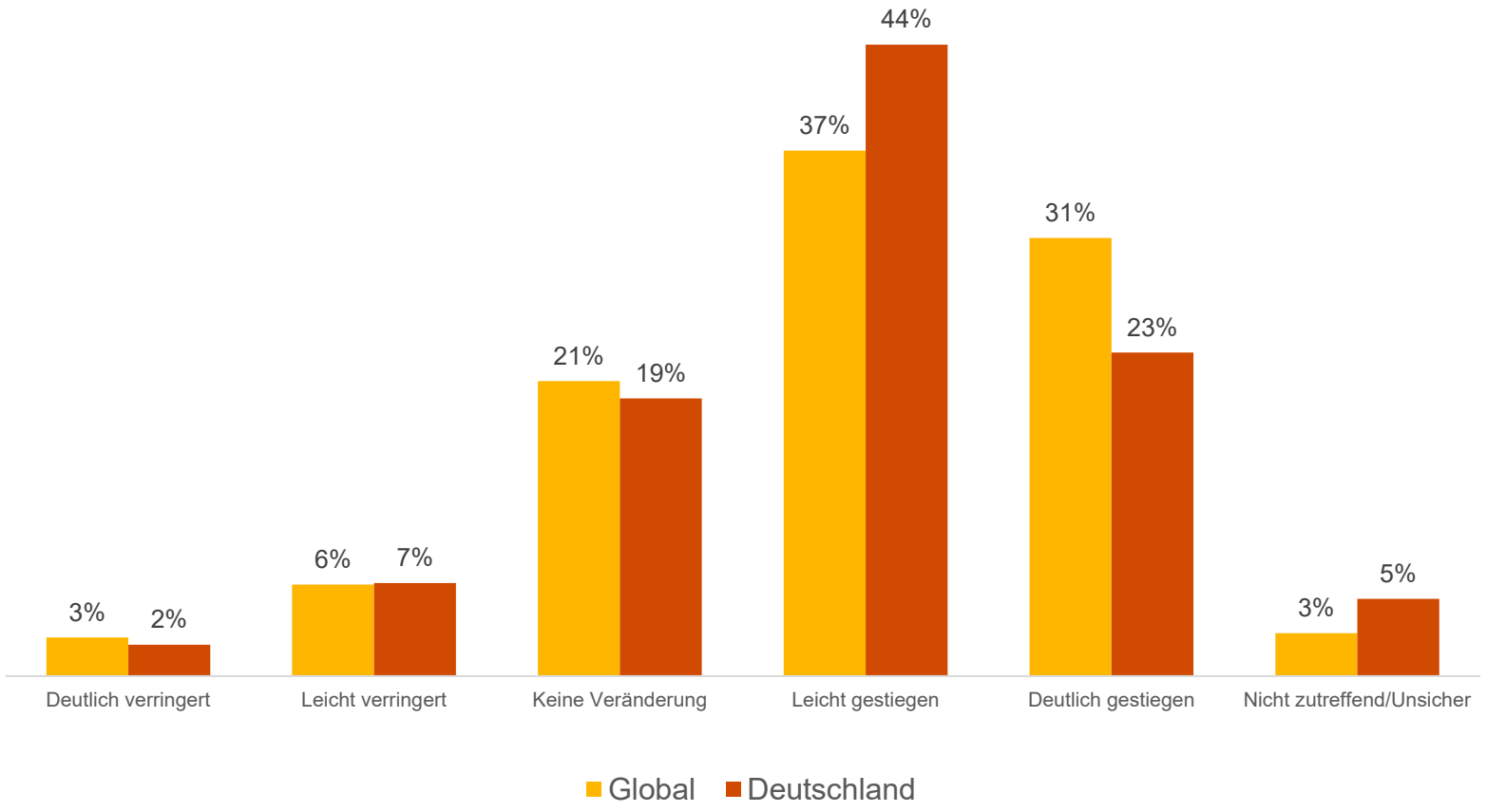
3

Der Einfluss generativer KI

Generative KI vergrößert die Angriffsfläche

Die zunehmende Komplexität und Dynamik von KI-Systemen erschwert es, potenzielle Schwachstellen zu identifizieren und abzusichern. Zudem erfordert die sichere Integration und Verwaltung der Technologie spezialisierte Fachkenntnisse, die oft fehlen. So hat sich die Angriffsfläche durch GenAI bei den befragten Unternehmen meist vergrößert.

GenAI verändert IT-Umgebungen und erhöht die Komplexität von Abwehrmaßnahmen



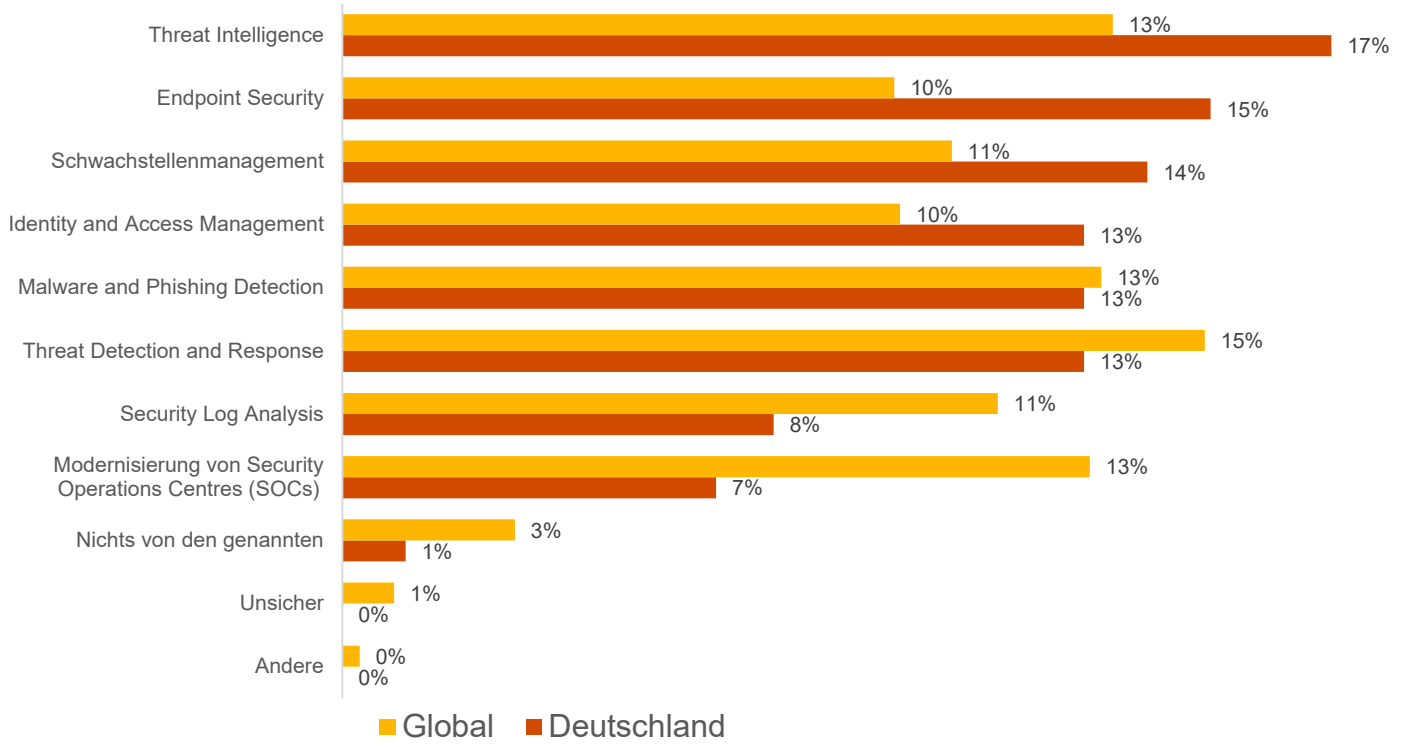
Fragestellung: Inwieweit hat generative KI die Angriffsfläche für Cyberangriffe in Ihrer IT-Umgebung in den letzten 12 Monaten beeinflusst? Basis: Sicherheitsverantwortliche (1762 Global / 93 Deutschland)

KI als Unterstützung für die Threat Intelligence

Generative KI erhöht nicht nur die Angriffsfläche, sondern stärkt richtig eingesetzt auch die Cyberabwehr. Unternehmen kennen diesen Vorteil – und planen, ihn in den nächsten Monaten für sich zu nutzen.

> Viele der befragten Unternehmen planen, GenAI zugunsten ihrer Cyberabwehr einzusetzen. Sicherheitsverantwortliche aus Deutschland wollen dabei vor allem den KI-Einsatz für Threat Intelligence, Sicherheit von Endgeräten und Schwachstellen-management priorisieren.
>
> Grant Waterfall, Cyber Security & Privacy Leader bei PwC Deutschland und EMEA

Generative KI kann die Cyberabwehr stärken und den Cyberschutz verbessern

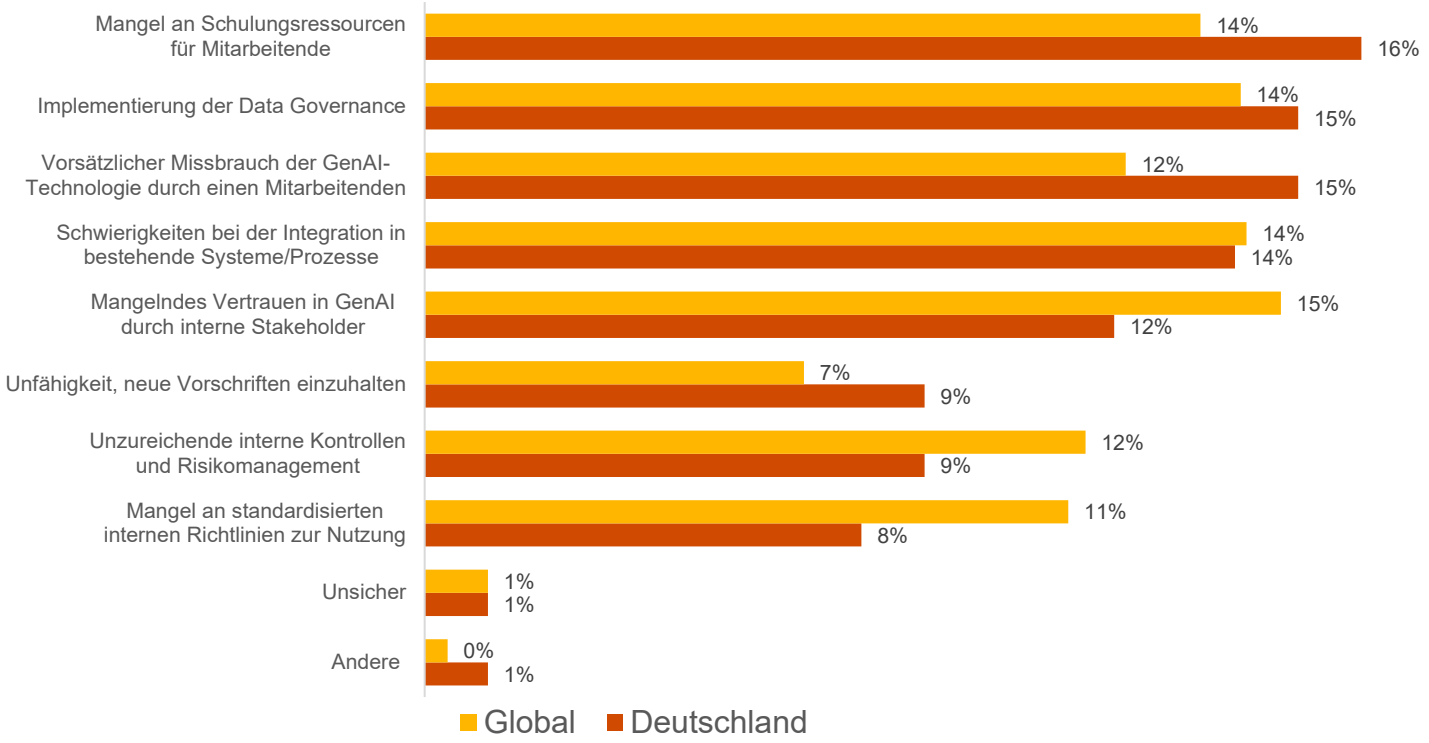


Fragestellung: In welchen Bereichen der Cyberabwehr wird Ihre Organisation in den nächsten 12 Monaten vorrangig generative KI einsetzen? Basis: Sicherheitsverantwortliche (1762 Global / 93 Deutschland)

KI-Schulungen stellen Unternehmen vor Herausforderungen

Die Integration von generativer KI in die Sicherheitsinfrastrukturen ist ein komplexes Unterfangen, allen voran in Bezug auf die Schulung von Mitarbeitenden oder der Implementierung von Data Governance.

GenAI als Herausforderung für Cybersicherheit und Datenschutz



Fragestellung: Welche sind die größten Herausforderungen, denen sich Ihr Unternehmen in Bezug auf generative KI im Zusammenhang mit Cybersicherheit und Datenschutz in den nächsten 12 Monaten stellen muss? Basis: Sicherheitsverantwortliche mit Ausnahme derjenigen, die dem Einsatz von GenAI in der Cyberverteidigung keine Priorität einräumen oder sich nicht sicher sind (1694 Global / 92 Deutschland)

4

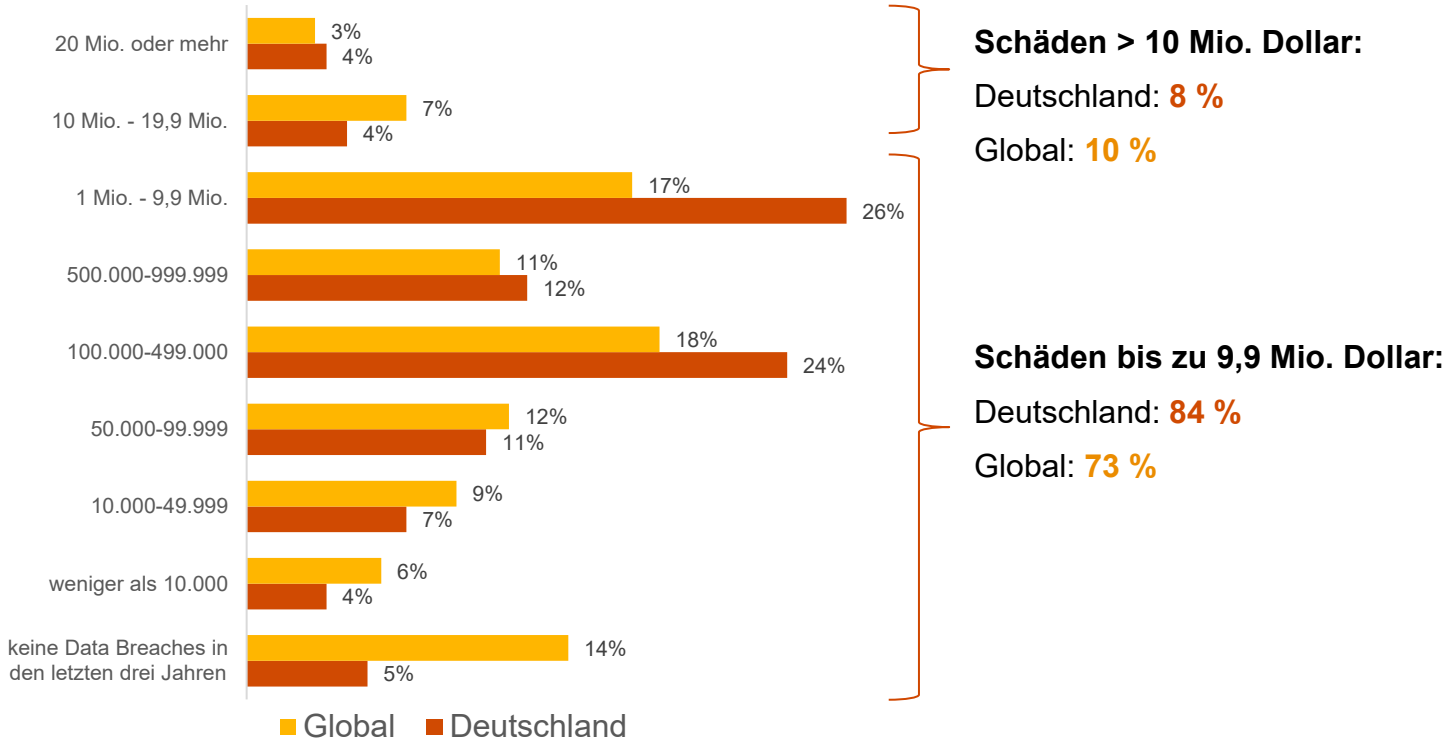
Cyberresilienz und Risiko-quantifizierung

Hohe Kosten durch Datendiebstahl und -missbrauch

Cybersicherheit stellt nicht nur ein operatives Risiko dar, sondern hat auch finanzielle Auswirkungen: 84 % der befragten deutschen Unternehmen entstanden durch den schwersten Fall von Datendiebstahl und -missbrauch Kosten bis zu 9,9 Mio. Dollar. Ein Viertel verzeichnete Schäden zwischen einer und knapp zehn Millionen US-Dollar.

Bedenklich: In Deutschland berichteten nur 5 % der Befragten, zuletzt keine Data Breaches erlitten zu haben (weltweit: 14 %).

Kosten der schwersten Data-Breach-Vorfälle in den letzten drei Jahren (US-Dollar)



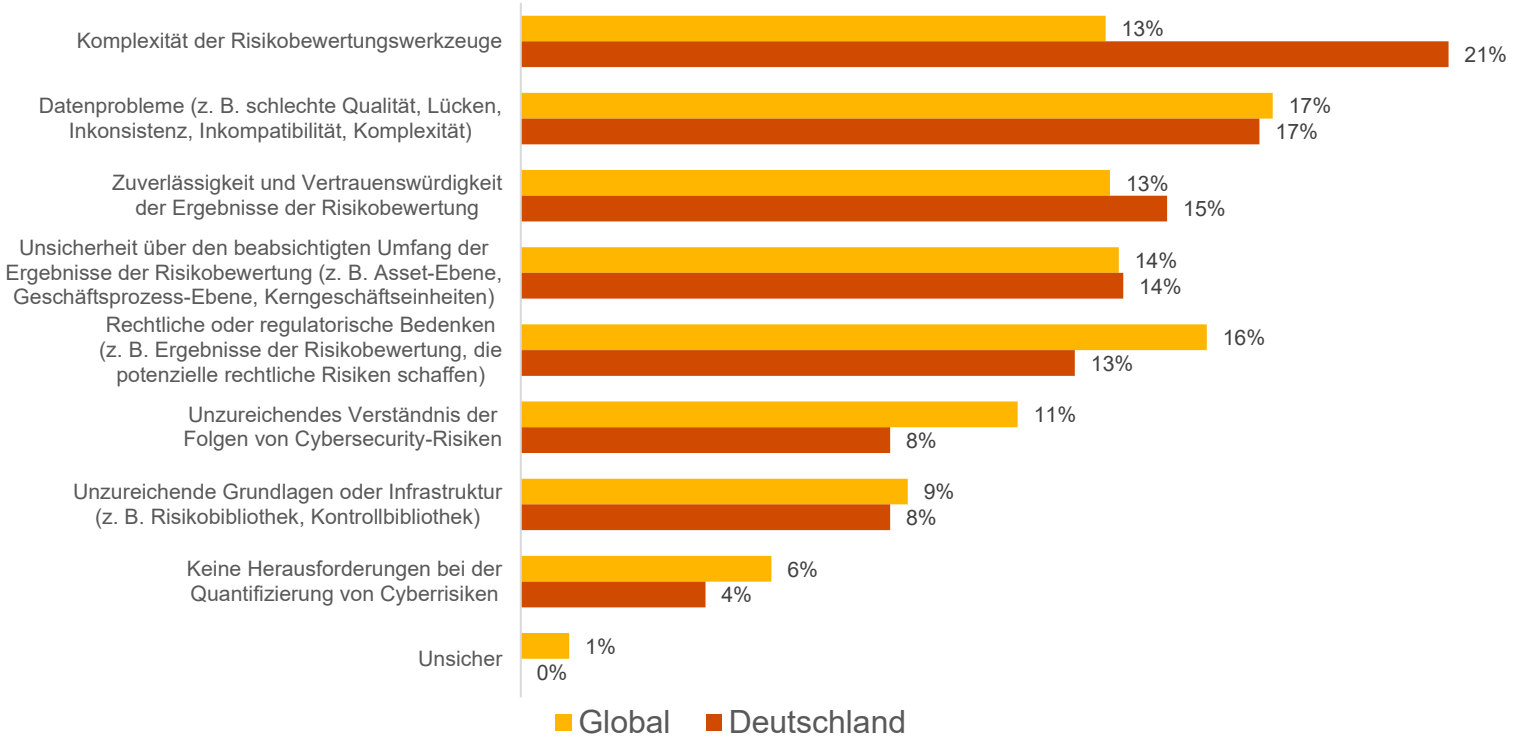
Fragestellung: Bitte schätzen Sie die Kosten für Ihre Organisation beim größten schädlichen Data Breach in den letzten drei Jahren ein. Basis: Security und CFOs (1951 Global / 114 Deutschland)

Risikoquantifizierung ist in vielen Unternehmen noch lückenhaft

Durch die Quantifizierung von Risiken können Organisationen fundierte Entscheidungen treffen, effektive Sicherheitsmaßnahmen implementieren und Ressourcen gezielt einsetzen, um die Wahrscheinlichkeit und den Schaden von Cyberangriffen zu minimieren.

Auffällig: In Deutschland gibt es erhöhte Herausforderungen mit der Komplexität von Risikobewertungswerkzeugen.

Herausforderungen bei der Quantifizierung potenzieller finanzieller Auswirkungen von Cyberrisiken (Top-Nennung)

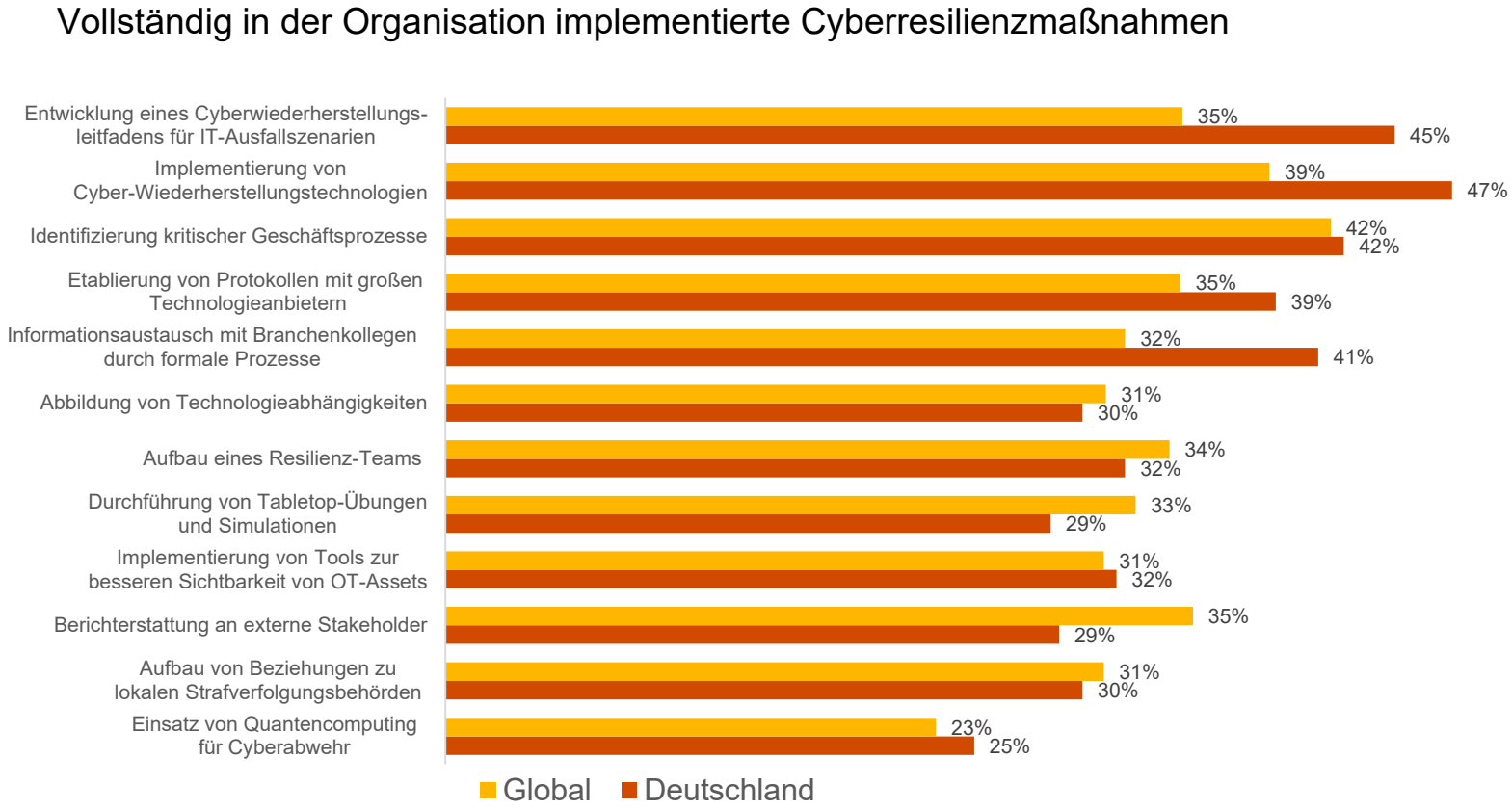


Fragestellung: Vor welchen Herausforderungen stand Ihr Unternehmen, wenn überhaupt, bei der Quantifizierung der potenziellen finanziellen Auswirkungen von Cyberrisiken?
Basis: Sicherheitsverantwortliche, CEOs, Board Member, CFOs und CROs, die Risikoquantifizierung betreiben. (1899 Global / 95 Deutschland)

Maßnahmen zur Verbesserung der Cyberresilienz sind noch ausbaufähig

Viele Unternehmen haben wichtige Initiativen zur Stärkung ihrer Cyber-resilienz erst teilweise oder noch gar nicht umgesetzt. Besonders bedenklich, um im Krisenfall einsatzbereit zu sein: Nur **32 % haben ein Resilienz-Team** unter Berücksichtigung aller Geschäftsbereiche aufgebaut.

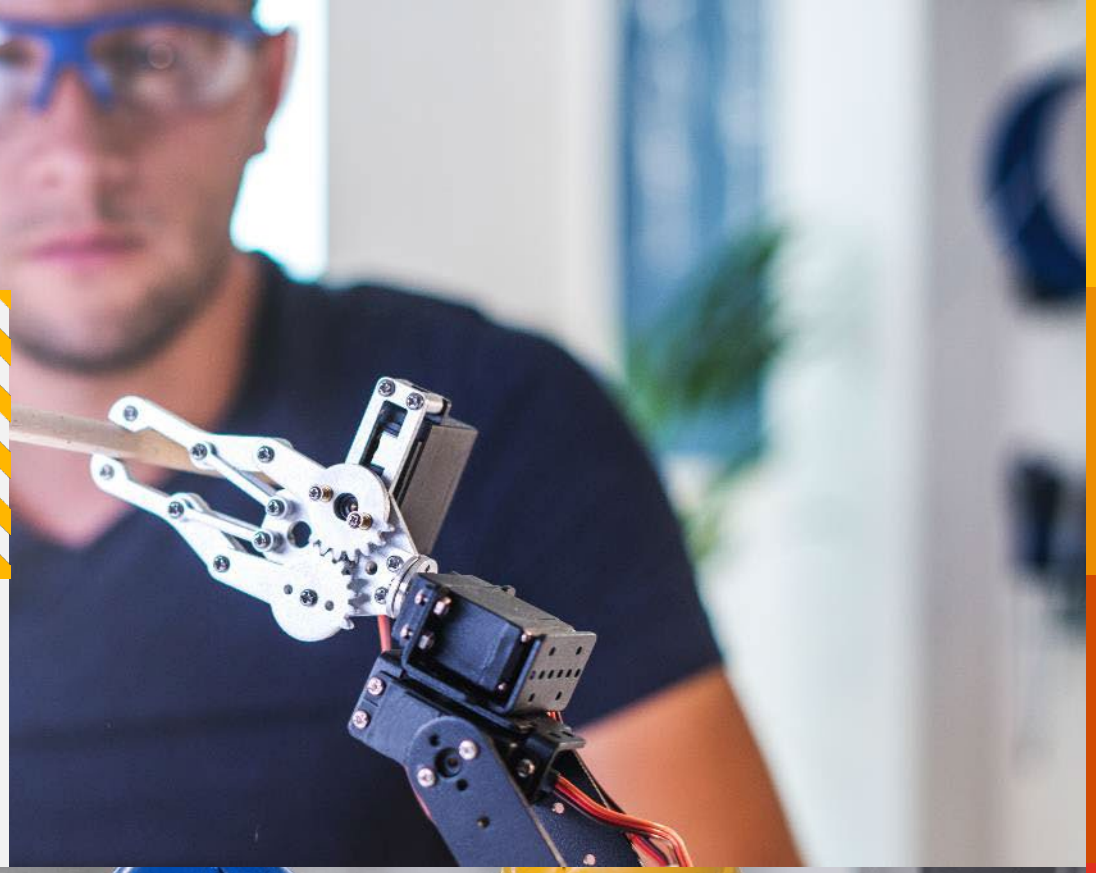
Bei Recovery-Planungen und -Technologien ist Deutschland hingegen vergleichsweise weit, genauso wie beim Informations-austausch mit der Fach-Community.



Fragestellung: Inwieweit führt Ihre Organisation die folgenden Maßnahmen zur Verbesserung der Cyberresilienz durch? Basis: Alle Unternehmen (4042 Global / 253 Deutschland)

5

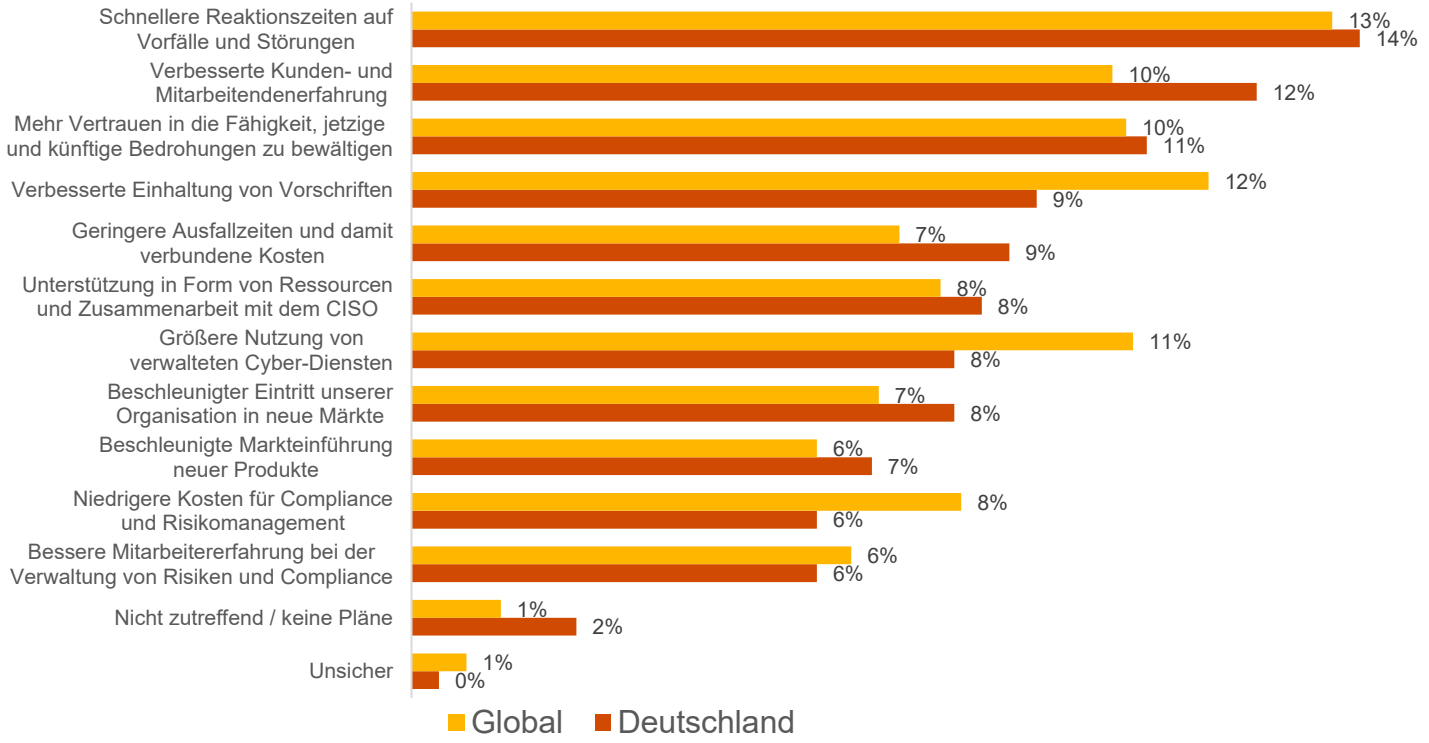
Strategische Ziele und Leadership



Ambitionierte Ziele für Sicherheit und Datenschutz

Unternehmen streben mit Blick in die Zukunft vor allem schnellere Reaktionszeiten auf Sicherheitsvorfälle und Störungen an – dies ist in Anbetracht der wachsenden Schäden durch Cybervorfälle und -störungen die richtige Priorität.

Strategie-, Mitarbeitenden- und Investitionsziele in den nächsten 12 Monaten (Top-Nennung)



Fragestellung: Welche Strategie-, Mitarbeitenden- und Investitionsziele verfolgt Ihr Unternehmen in den nächsten 12 Monaten in Bezug auf Cyber- und Datenschutz? Basis: Alle Unternehmen (4042 Global / 253 Deutschland)

Cybersicherheit bleibt Chefsache, Involvierung von CISOs und Vorstands-Expertise ausbaufähig

Führungskräfte stehen vor der Herausforderung, das Vertrauen in ihre Fähigkeiten zur stärken.

nur 45 %

der deutschen CISOs spielen eine aktive Rolle bei der strategischen Planung von Cyberinvestitionen mit dem CFO.

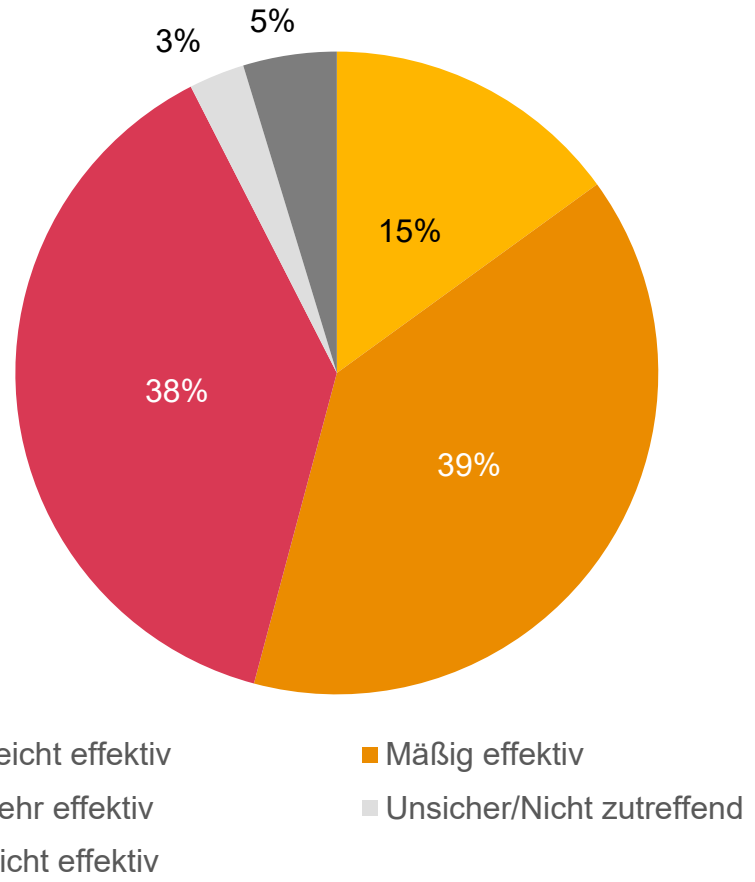
16 %

der deutschen CEOs sind vor allem in die Erörterung der wichtigsten Kennzahlen auf Board-Ebene involviert.

5 %

meinen, dass die Cyberexpertise im Vorstand ihrer Organisation nicht effektiv ist.

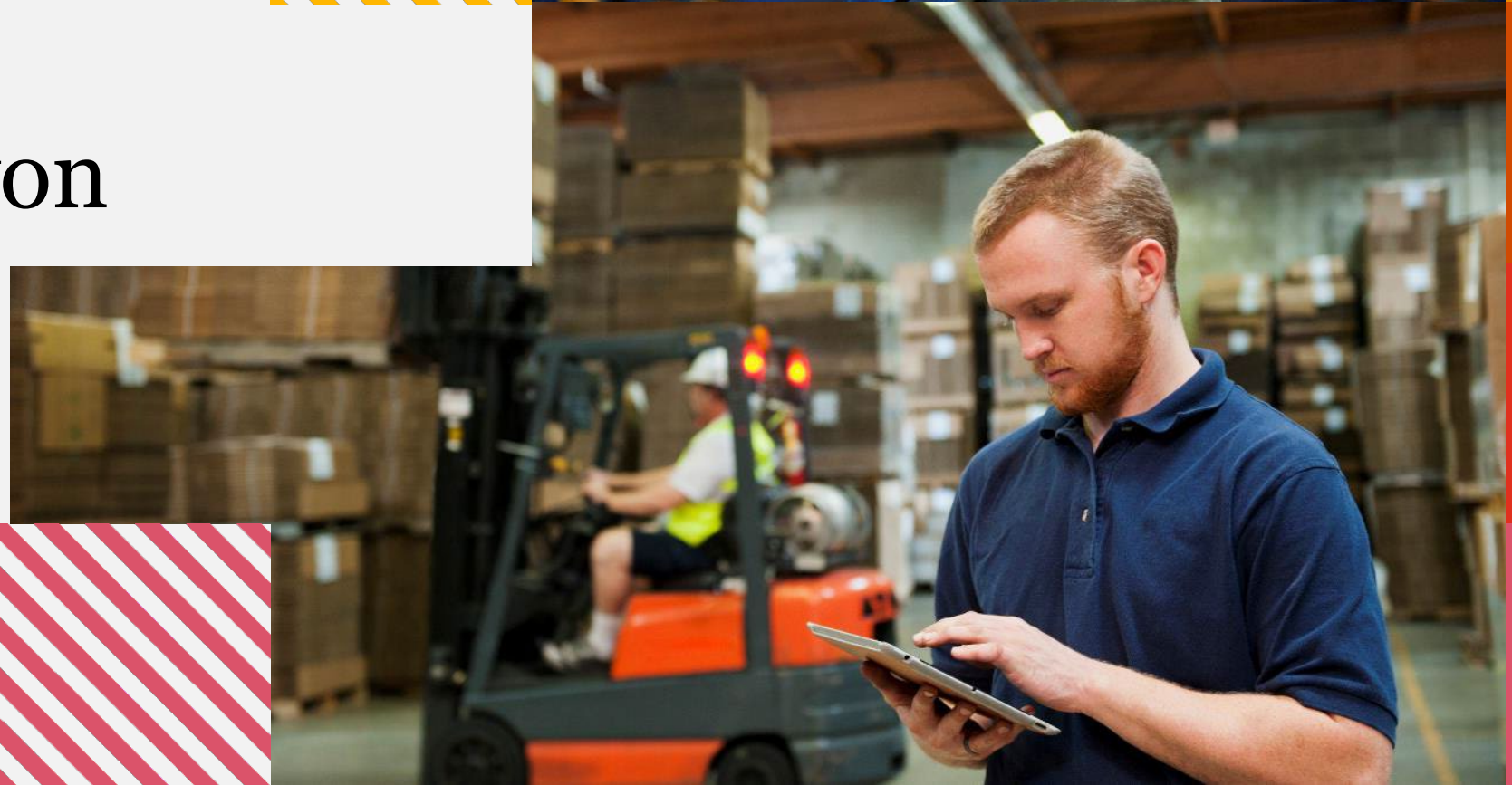
Effektivität der Cyberexpertise im Vorstand



Fragestellungen: Wie stark nimmt Ihr CISO eine aktive Rolle in strategischer Planung mit dem CFO bzgl. Cyber-Investitionen ein? Basis: Alle außer CISO (203 Deutschland) / Wie stark ist Ihr CEO in die folgenden Cyber- und Datenschutzangelegenheiten involviert? Basis: Alle außer CEOs (232 Deutschland) / Für wie effektiv halten Sie die Cyberexpertise in Ihrem Vorstand? Basis: Alle Unternehmen (196 Deutschland)

6

Auswirkungen von Regulatorik



Regulierung in Deutschland oft hilfreich, aber auch herausfordernd

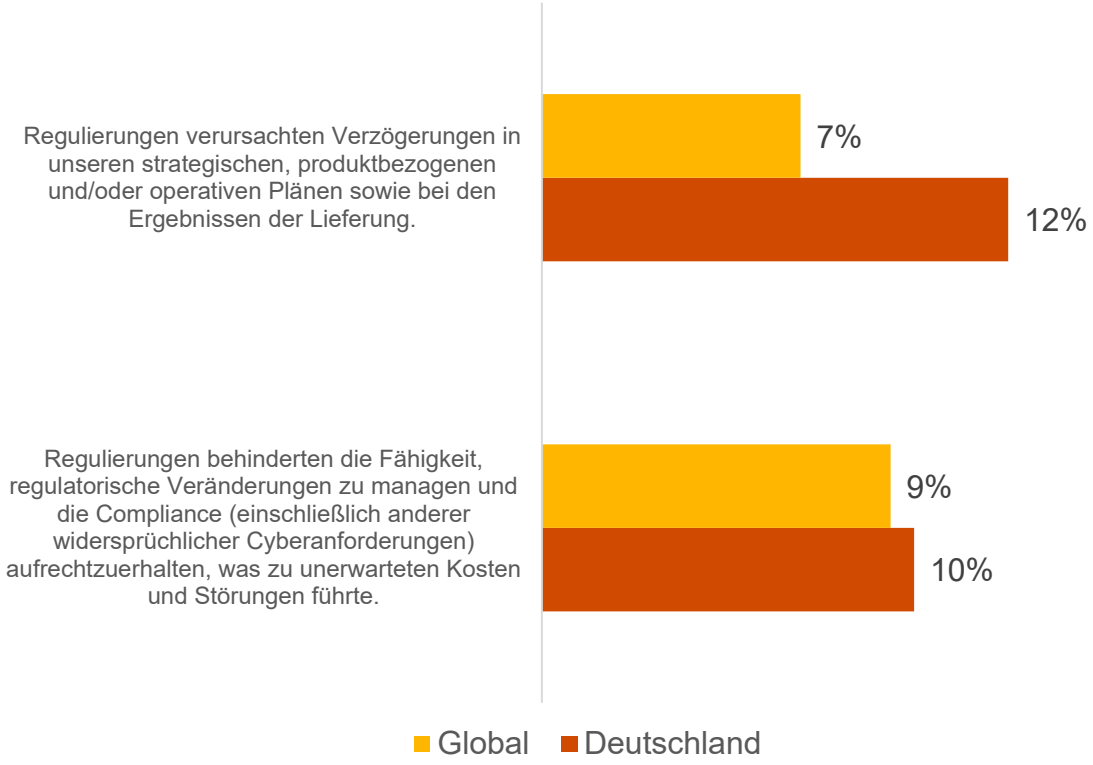
Cyber-Security-Regulierungen haben 73 % der Organisationen geholfen – aber bei 21 % waren die Herausforderungen groß:

21 %
Regulierungen halfen unserer Organisation resilienter zu werden, indem sie einen branchenweiten Rahmen vorgegeben haben.

21 %
Regulierungen halfen unserer Organisation, Leitplanken für Technologieinnovationen und Transformationsbemühungen zu etablieren.

16 %
Regulierungen führten dazu, dass wir Cyber Managed Services in Betracht zogen, um regulatorische Anforderungen zu erfüllen.

15 %
Regulierungen haben uns herausgefordert, das aktuelle Cyber-Risiko-management-Programm, Prozesse und Governance-Ansätze zu stärken.



Fragestellung: Welche Aussage, wenn überhaupt, spiegelt die Auswirkungen neuer Cybersicherheitsvorschriften auf Ihr Unternehmen in den letzten 12 Monaten am besten wider? Basis: Alle Unternehmen (4042 Global, 253 Deutschland)

7

Über die Studie

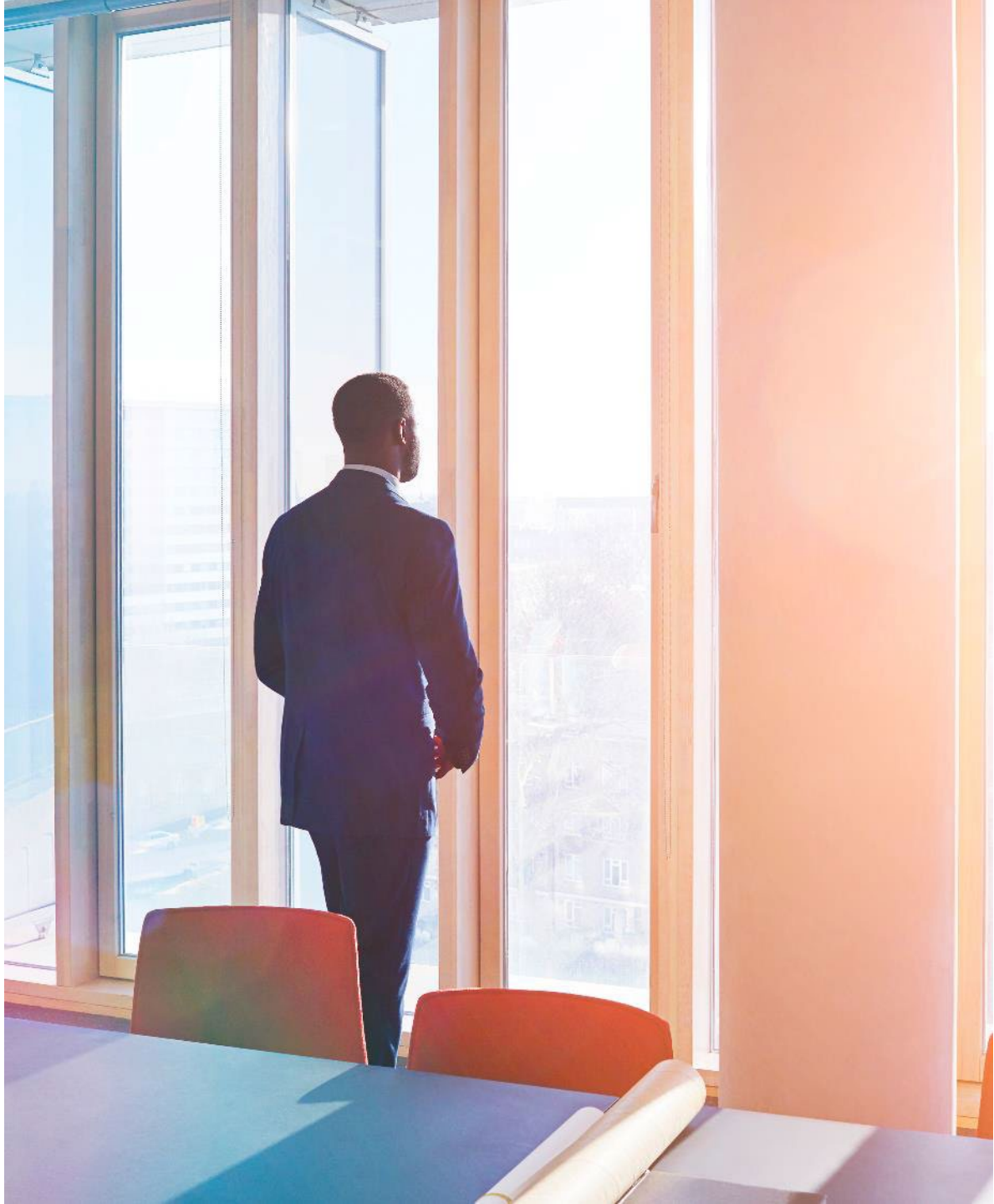
Über die Studie

Die PwC-Studie Global Digital Trust Insights (DTI) 2025 ist eine Umfrage unter 4.042 Geschäfts- und Technologie-Führungskräften, die im Zeitraum von Mai bis Juli 2024 durchgeführt wurde. Ein Viertel der Führungskräfte stammt aus großen Unternehmen mit einem Umsatz von 5 Milliarden US-Dollar oder mehr. In Deutschland wurden 253 Unternehmen befragt.

Die Global Digital Trust Insights Survey war früher als Global State of Information Security Survey (GSISS) bekannt. Sie findet nun bereits zum 27. Mal statt und ist die am längsten laufende jährliche Umfrage zu Cybersecurity-Trends. Zudem ist sie die größte Umfrage in der Cybersecurity-Branche und die einzige, an der nicht nur Sicherheits- und Technologie-Führungskräfte, sondern auch leitende Business-Führungskräfte teilnehmen.

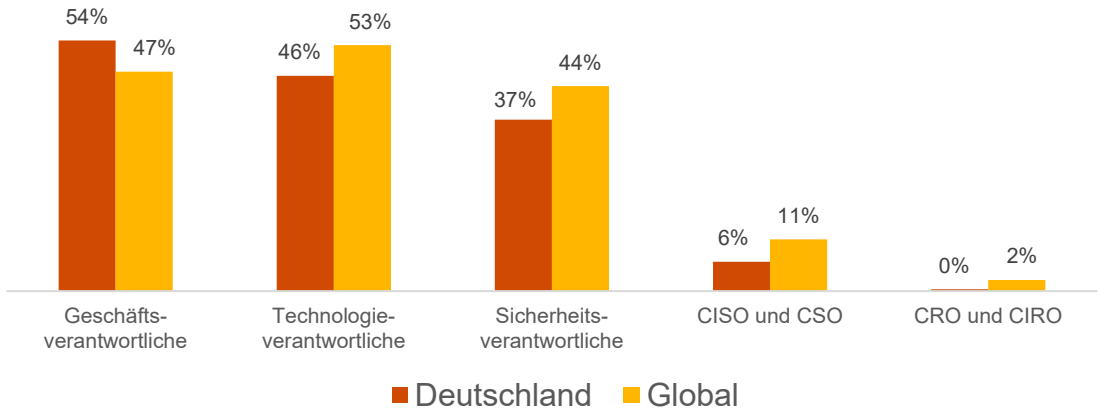
Die Umfrage wurde von PwC Research durchgeführt, einem globalen Kompetenzzentrum von PwC für Marktforschung und Insights.

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

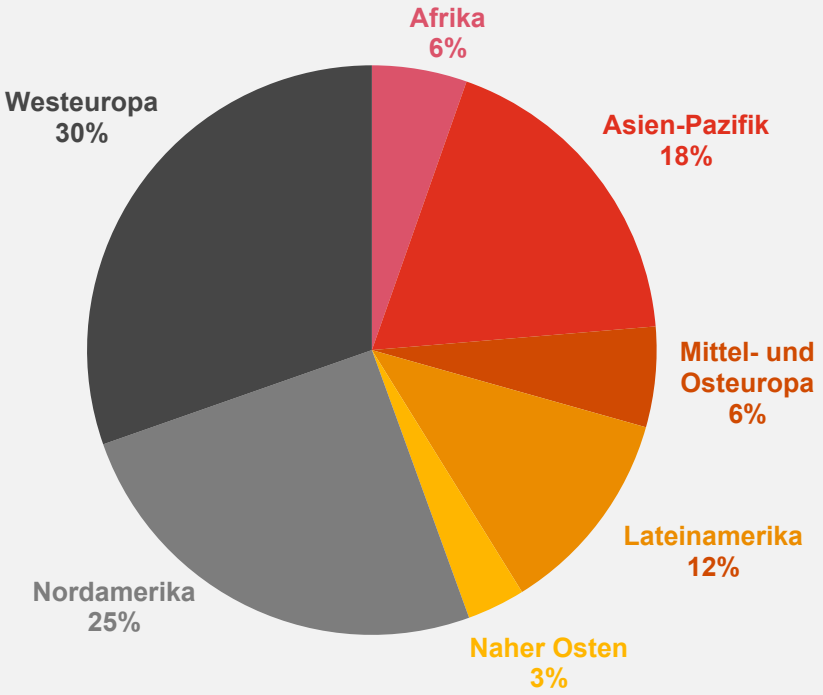


Stichprobe

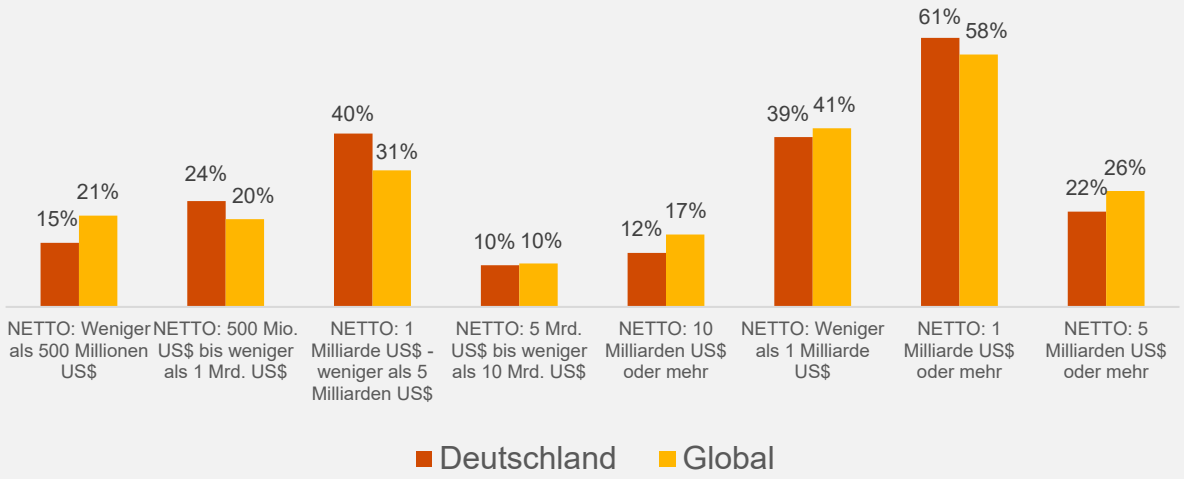
Jobtitel



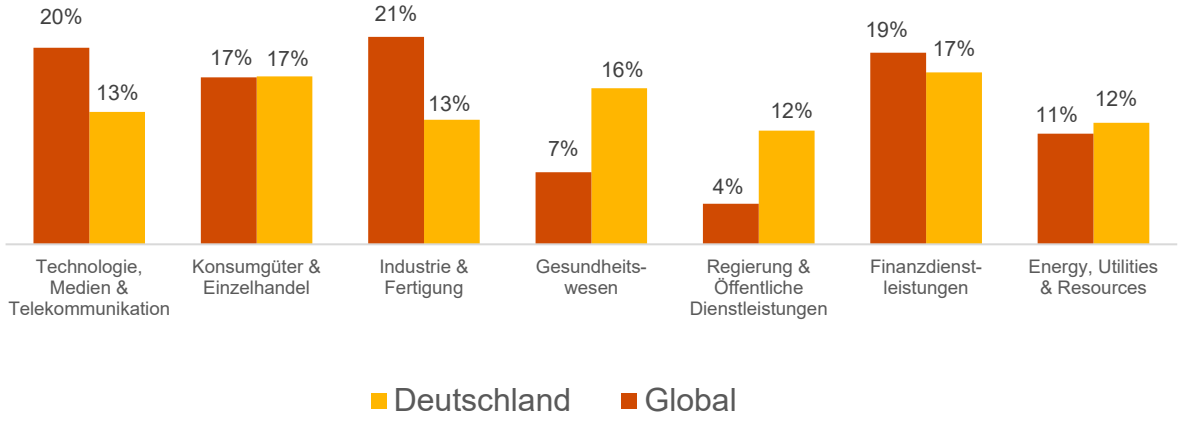
Region



Umsatz



Branchen



Vielen Dank

pwc.de/cybersecurity