Weltweite Studie zum Thema Security 2024

Ergebnisse weltweit

November 2024

Durchführung der Studie:
SAPIO Research

Übersicht und Methodik

Die Umfrage wurde unter 1.800 Entscheidern aus dem Bereich der Cybersicherheit (über 2/3 der Befragten treffen direkte Entscheidungen zum Thema Cybersicherheit oder haben Einfluss auf diese Entscheidungen) in Unternehmen mit mehr als 500 Mitarbeitern (mehr als 250 Mitarbeitern in Australien und Neuseeland) durchgeführt. Die Studienteilnehmer decken ein breites Spektrum an Funktionen in den Bereichen IT, Operations und Obere Führungsriege ab.

Bezogen auf die Grundgesamtheit, liegen 50 % der Stichprobenergebnisse bei einem Konfidenzintervall von 95 % in einem Bereich von ±2,3 % um den wahren Wert.

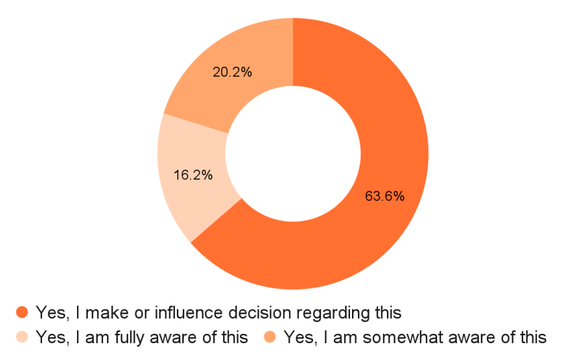
Die Befragungen wurden von Sapio Research im September 2024 per Onlineumfrage mittels E-Mail-Einladung durchgeführt.

Demografische Daten zu den Befragten – Entscheider im Bereich Cybersicherheit

Führungsgrad

Abteilung	% der Befragten
IT	51 %
Operations	27 %
Obere Führungsriege	22 %

Entscheidungskompete



Führungsgrad

Anz. Beschäftigte	% der Befragten
250-999	22 %
1.000-4.999	35 %
5.000-24.999	26 %
>25.000	17 %

Primärer Wirtschaftszweig

1. Groß- und Einzelhandel – 12 %
2. Technologie – 11 %
3. Finanzen / Buchhaltung – 11 %
4. Gesundheit / Life Sciences – 11 %
5. Medien / Unterhaltung / Reisen und Tourismus – 11 %
6. Regierung / Öffentlicher Sektor – 11 %

Wohnsitzland

Skandinavien

LATAM

UK & Irland

Japan

DACH

AUS & NZ

USA

Spanien

Frankreich

Fazit

Wichtige Statistiken

Für die Erholung von Sicherheitsvorfällen werden von Unternehmen **5,85 Monate** veranschlagt.

Unternehmen waren im vergangenen Jahr im Durchschnitt von rund **40** Sicherheitsvorfällen betroffen. Die wichtigsten Ursachen waren dabei **externe Angreifer (38 %)** und **Softwarefehler (33 %)**.

Unternehmen verlassen sich auf durchschnittlich **8** Cybersicherheitslösungen, wobei sich die Hauptfunktionen dieser Lösungen zu **38 %** überschneiden.

Unternehmen gehen davon aus, dass **Social-Engineering-Angriffe (37 %)** sowie **Ransomware und Erpressung (34 %)** in den nächsten 12 Monaten die größten Bedrohungen für ihre Cybersicherheit darstellen werden.

Umsatzeinbußen gehörten zu den Hauptfolgen von Sicherheitsvorfällen **(23 %)**, wobei der durchschnittliche Verlust **2,9 %** betrug.

Fast drei Viertel (73 %) geben an, dass eine Konsolidierung von Sicherheitslösungen aufgrund immer knapperer Budgets **für sie attraktiver sei**.

Zusammenfassung und Übersicht

1. **Reaktion auf jüngste Sicherheitsvorfälle:** Nach jüngsten Sicherheitsvorfällen gehen Unternehmen **vorsichtiger** mit Updates und Patches um. Wir beobachten eine Fortsetzung dieses Trends, wenn es um eine Neubewertung der aktuellen Anbieter und Tools für die Cybersicherheit geht. Eine Reihe von Unternehmen ziehen sogar einen **Anbieterwechsel** in Betracht. Dies verdeutlicht die Ängste der Unternehmen, die versuchen, sich inmitten sich ständig weiterentwickelnder Sicherheitsbedrohungen zurechtzufinden. Die Erholung von Sicherheitsvorfällen ist **langwierig** und bedarf eines hohen Ressourcenaufwands.

2. **Auswirkungen und Folgen von Sicherheitsvorfällen**: Unternehmen waren in den vergangenen 12 Monaten im Durchschnitt von **40 Sicherheitsvorfällen** betroffen. Die wichtigsten Ursachen waren dabei externe Angreifer und Softwarefehler. Die größten Auswirkungen solcher Vorfälle sind **Ausfallzeiten** und **Datenverluste**. Umsatzeinbußen von durchschnittlich **2,9 %** gehören ebenfalls zu den häufigsten Auswirkungen, was die finanziellen Folgen unzureichender Sicherheitsmaßnahmen verdeutlicht. Trotz dieser Herausforderungen ergreifen Unternehmen proaktive Schritte, um ihren Sicherheitsstatus nach Vorfällen zu verbessern. Ein besonderer Schwerpunkt liegt dabei auf der **Schulung von Mitarbeitern, um Kompetenzlücken zu schließen**. Diejenigen Unternehmen, die von DDoS-Angriffen betroffen sind, fühlen sich bei der Bewältigung solcher Angriffe **schlecht vorbereitet**. Die zunehmende Automatisierung und Qualifikationslücken im Bereich der generativen KI geben weiterhin **erheblichen Anlass** zur Sorge.

3. **Das aktuelle Cybersicherheitsumfeld und zukünftige Bedrohungen:** Cybersicherheitsexperten zufolge werden Social-Engineering-Angriffe in Zukunft die größte Bedrohung darstellen, dicht gefolgt von Ransomware und Erpressung. Dies zeigt eine deutliche Verlagerung hin zu **menschenzentrierten Schwachstellen**, bei denen Angreifer **psychologische Faktoren** ausnutzen. Die wichtigsten Ursachen für Cybersicherheitsbedrohungen lassen sich auf die **Entwicklungen im digitalen Umfeld** zurückführen. Dies zeigt auch, wie wichtig es ist, dass die Cybersicherheitslösungen von Unternehmen in der Lage sind, **auf dynamische Bedrohungen zu reagieren**.

Zusammenfassung und Übersicht

4. **Verschiebungen der Zuständigkeiten:** In Unternehmen herrscht weiterhin Unklarheit darüber, wer genau für Cybersicherheitsvorfälle verantwortlich ist. Die zunehmende teamübergreifende Zuständigkeit von Anwendungsentwicklern, Platform Engineers und Site Reliability Engineers deutet darauf hin, dass die Verantwortung für Cybersicherheitsvorfälle nicht länger ausschließlich auf Sicherheitsexperten beschränkt ist. Unternehmen haben im Allgemeinen ein gutes Gefühl für die Ressourcen, die für den Umgang mit Sicherheitsproblemen im gesamten Unternehmen zur Verfügung stehen. Remote-Mitarbeiter bleiben allerdings weiterhin gefährdet und es herrscht Nachholbedarf bei internen Schulungen.

5. **Investitionen in die Cybersicherheit**: Ein Großteil der Entscheider erwartet, dass ihre Investitionen im Hinblick auf die Cybersicherheit in den nächsten 12 Monaten **steigen** werden. Dies gilt insbesondere für Technologien wie **moderne Authentifizierungslösungen** und **Cyberversicherungen**. Diese Investitionen sind an den Umsatz- und Wachstumszielen der Unternehmen ausgerichtet, was zeigt, dass die **Cybersicherheit zunehmend in der strategischen Entscheidungsfindung berücksichtigt** wird. Es wird viel Geld in Tools investiert. Die Kehrseite davon ist allerdings, dass Unternehmen oft mehrere Sicherheitslösungen haben, deren Funktionen sich stark überschneiden.

6. **Konsolidierung von Sicherheitslösungen**: Unternehmen wünschen sich **mehr Kontrolle über ihre Sicherheit** und eine **bessere Integration von Tools und Daten**. Außerdem sind sie davon überzeugt, dass die Konsolidierung ihrer Sicherheitslösungen ihnen helfen wird, diese Ziele zu erreichen. Die Mehrheit der Befragten gab an, dass eine Konsolidierung **angesichts immer knapperer Budgets zunehmend attraktiver** wird. Eine Konsolidierung bringt aber auch Bedenken mit sich, insbesondere im Hinblick auf **mögliche Sicherheitslücken der Plattform** und potenziell **höhere Langzeitkosten**.

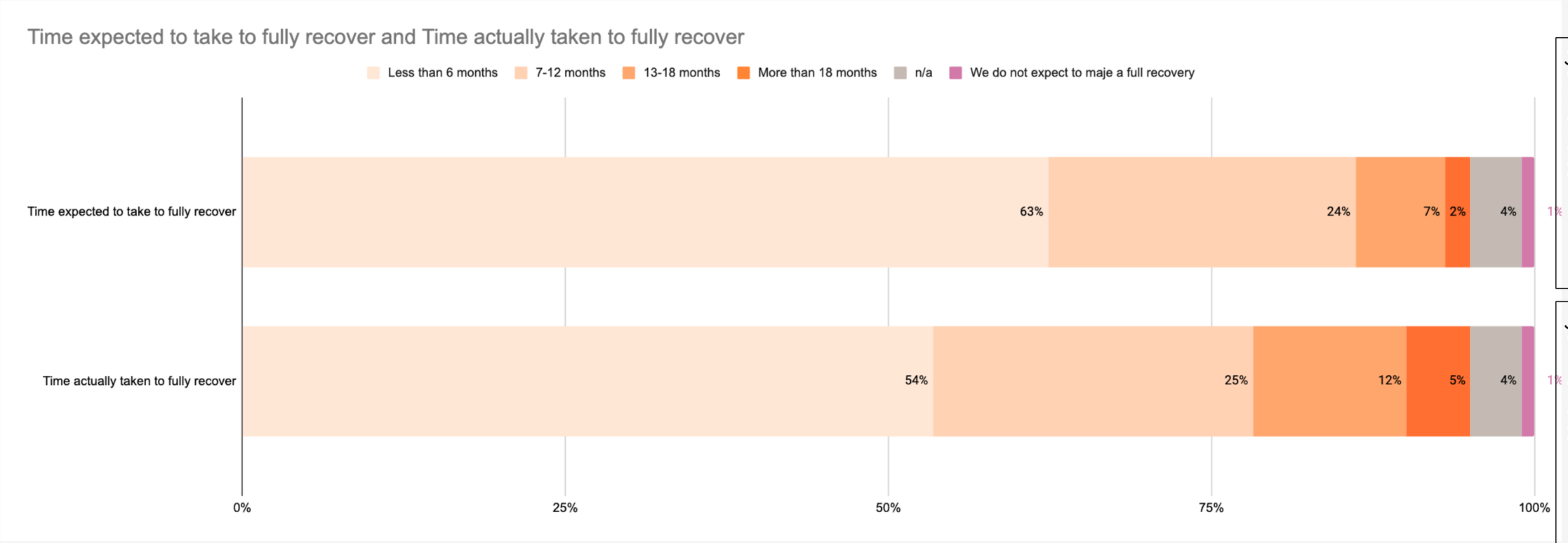
Wichtigste Ergebnisse

Wichtigste Ergebnisse

Reaktions- und Wiederherstellungszeit bei Sicherheitsvorfällen

Erwartete vs. tatsächliche Wiederherstellungszeit nach einem Sicherheitsvorfall

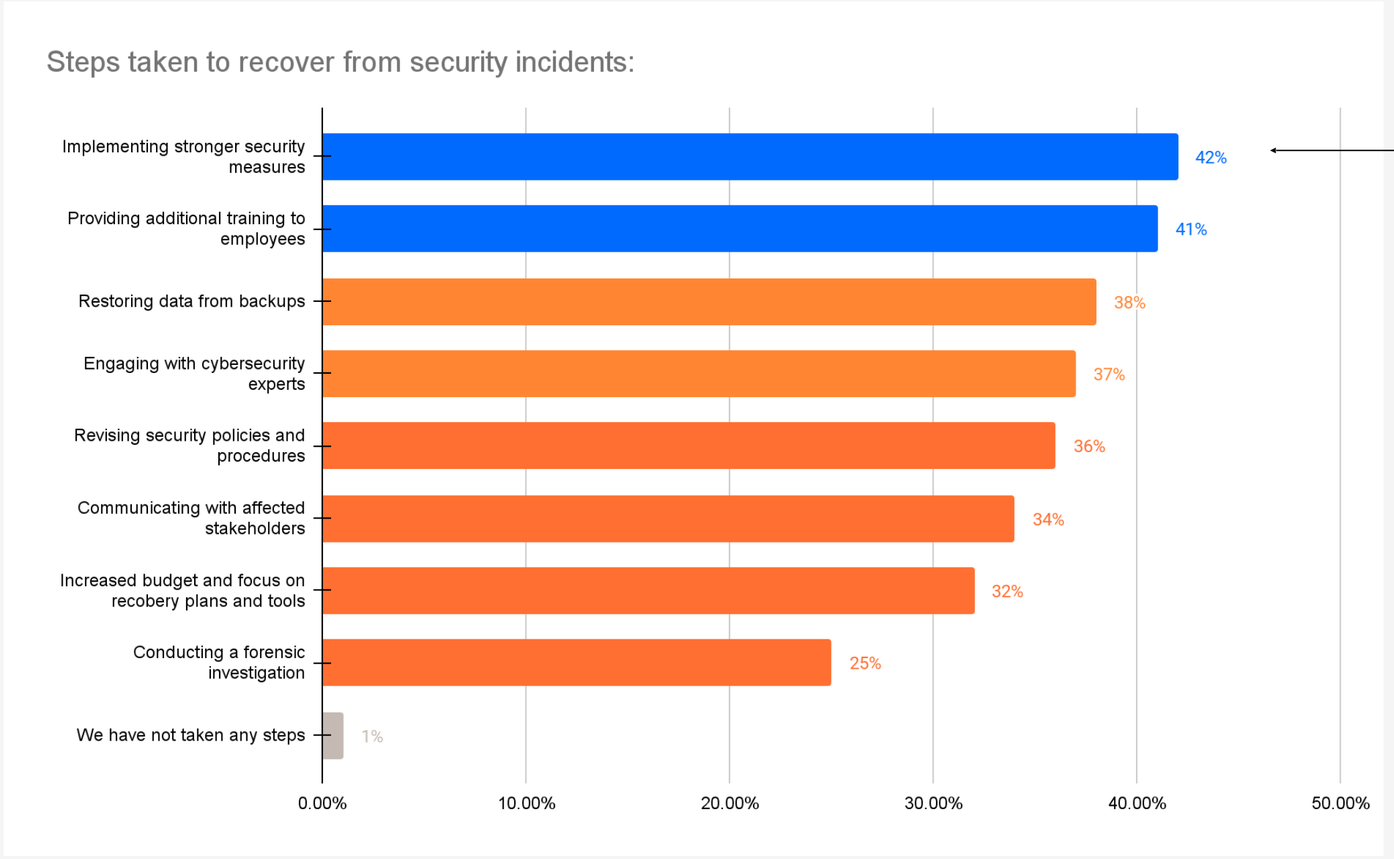
Die durchschnittliche Zeit, die Unternehmen benötigen, um sich von einem Sicherheitsvorfall zu erholen, beträgt **7 Monate** – 1 Monat länger als im Durchschnitt von Unternehmen erwartet.



F17e. Wie lange hat es gedauert, bis Sie sich von diesen Auswirkungen vollständig erholt hatten, oder wie lange wird es voraussichtlich dauern? I Basis: 1.632
* Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Schritte zur Erholung von Sicherheitsvorfällen

Die häufigsten Maßnahmen, die Unternehmen zur Erholung von Sicherheitsvorfällen ergreifen, sind **stärkere Sicherheitsmaßnahmen (43 %) und zusätzliche Mitarbeiterschulungen (41 %)**.



49 % Technologie
37 % Regierung / Öffentlicher Sektor

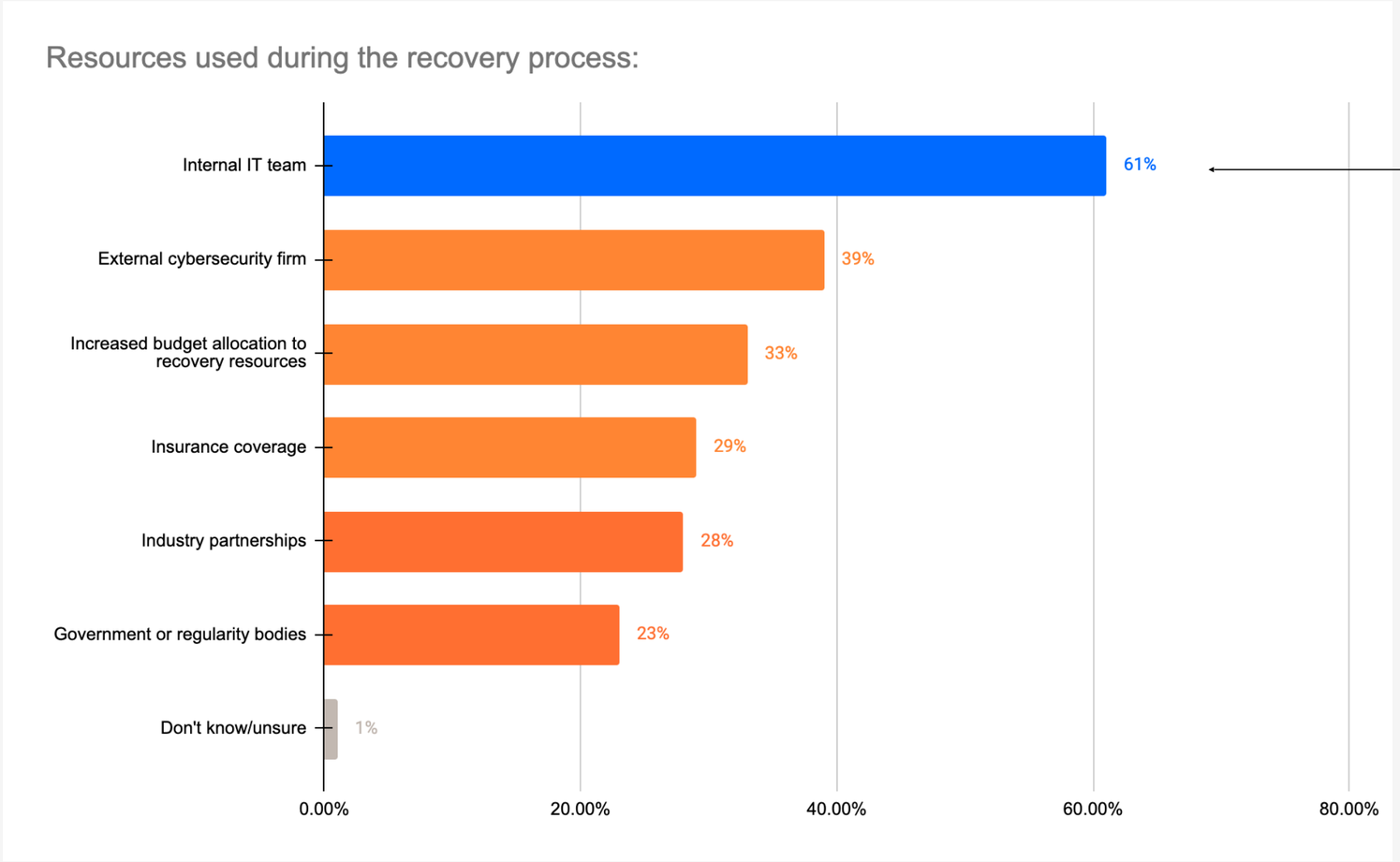
Unternehmen ergreifen proaktive Maßnahmen, um ihren Sicherheitsstatus nach Cybersicherheitsvorfällen zu verbessern.

Ein besonderer Schwerpunkt liegt dabei auf der Schulung von Mitarbeitern, um Kompetenzlücken zu schließen.

F18. Welche Schritte hat Ihr Unternehmen unternommen, um sich von dem Sicherheitsvorfall zu erholen? Bitte alle zutreffenden Antworten auswählen I Basis: 1.632 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Für die Erholung von Sicherheitsvorfällen aufgewendete Ressourcen

Die meisten Unternehmen setzen ihr **internes IT-Team (61 %)** bei der Erholung von Sicherheitsvorfällen ein.



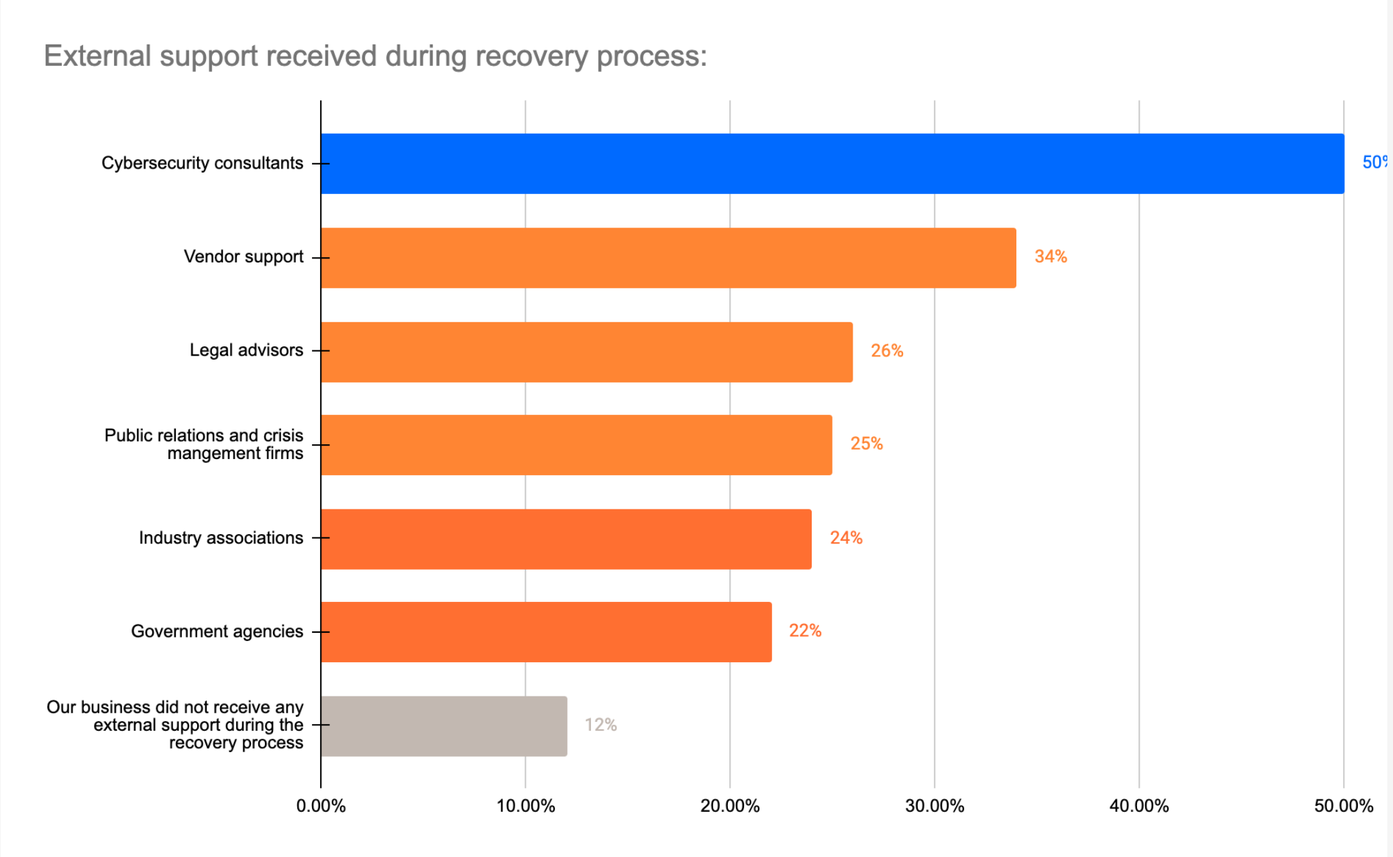
63 % in Unternehmen mit 250-999 Mitarbeitern
57 % in Unternehmen mit über 25.000 Mitarbeitern

Kleinere Unternehmen verlassen sich stärker auf interne Ressourcen.

F19. Welche Ressourcen hat Ihr Unternehmen bei der Erholung von Sicherheitsvorfällen genutzt? Bitte alle zutreffenden Antworten auswählen I Basis: 1.611 (Es wurden nur diejenigen Unternehmen befragt, die bereits Schritte zur Erholung von Sicherheitsvorfällen ergriffen hatten.)

Externe Unterstützung bei der Erholung von Sicherheitsvorfällen

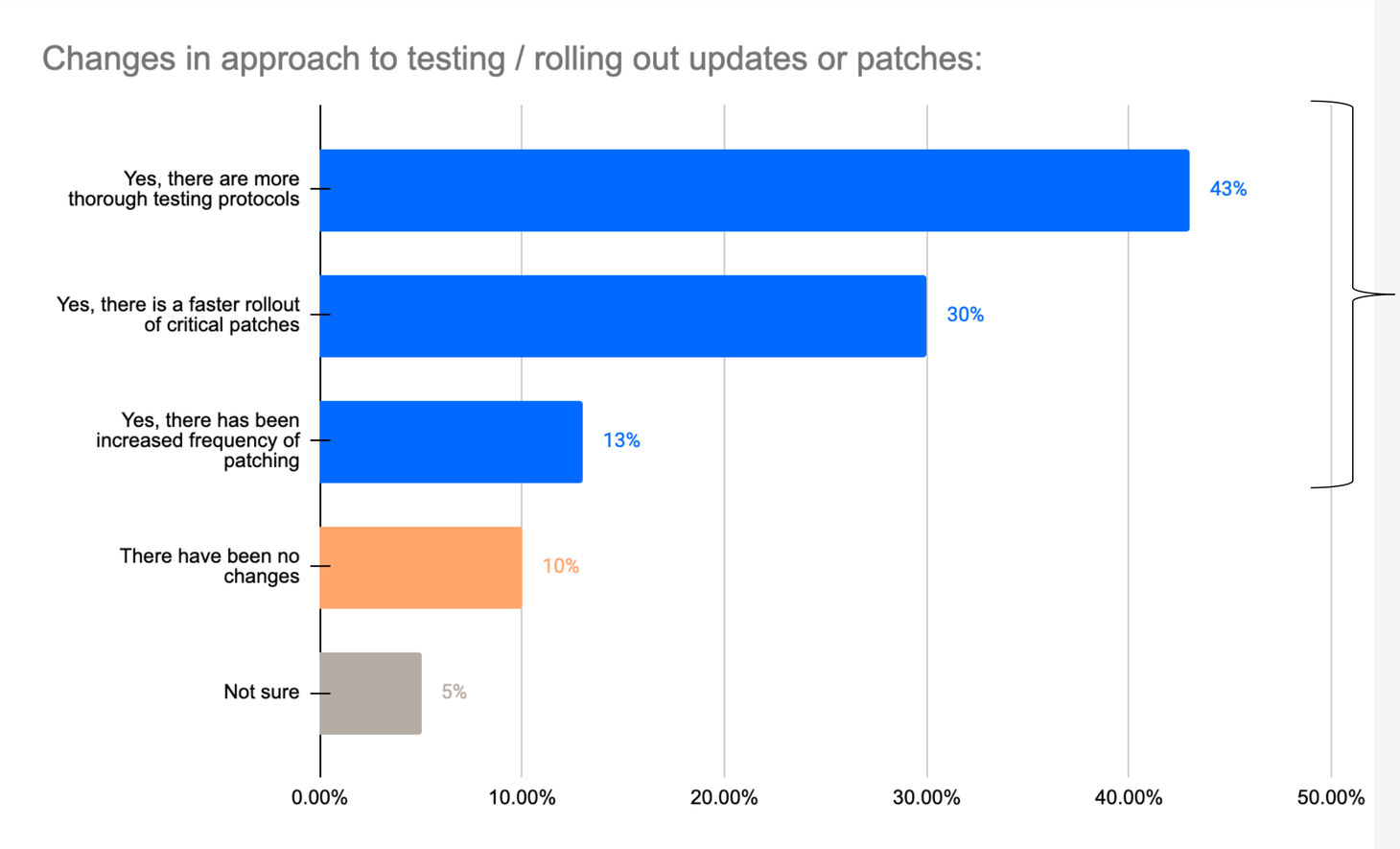
Etwa die **Hälfte** gibt an, dass ihr Unternehmen bei der Erholung von Sicherheitsvorfällen Hilfe von **Cybersicherheitsberatern** in Anspruch genommen hat.



F22b. Welche externe Unterstützung oder Hilfe hat Ihr Unternehmen bei der Erholung von Sicherheitsvorfällen erhalten (falls zutreffend)? Bitte alle zutreffenden Antworten auswählen I Basis: 1.800

Änderungen in der Vorgehensweise bei Updates und Patch-Tests

86 % der Befragten geben an, dass die jüngsten Probleme mit der Zuverlässigkeit ihr Unternehmen dazu veranlasst haben, ihre **Vorgehensweise beim Testen oder der Einführung von Updates oder Patches zu ändern**.



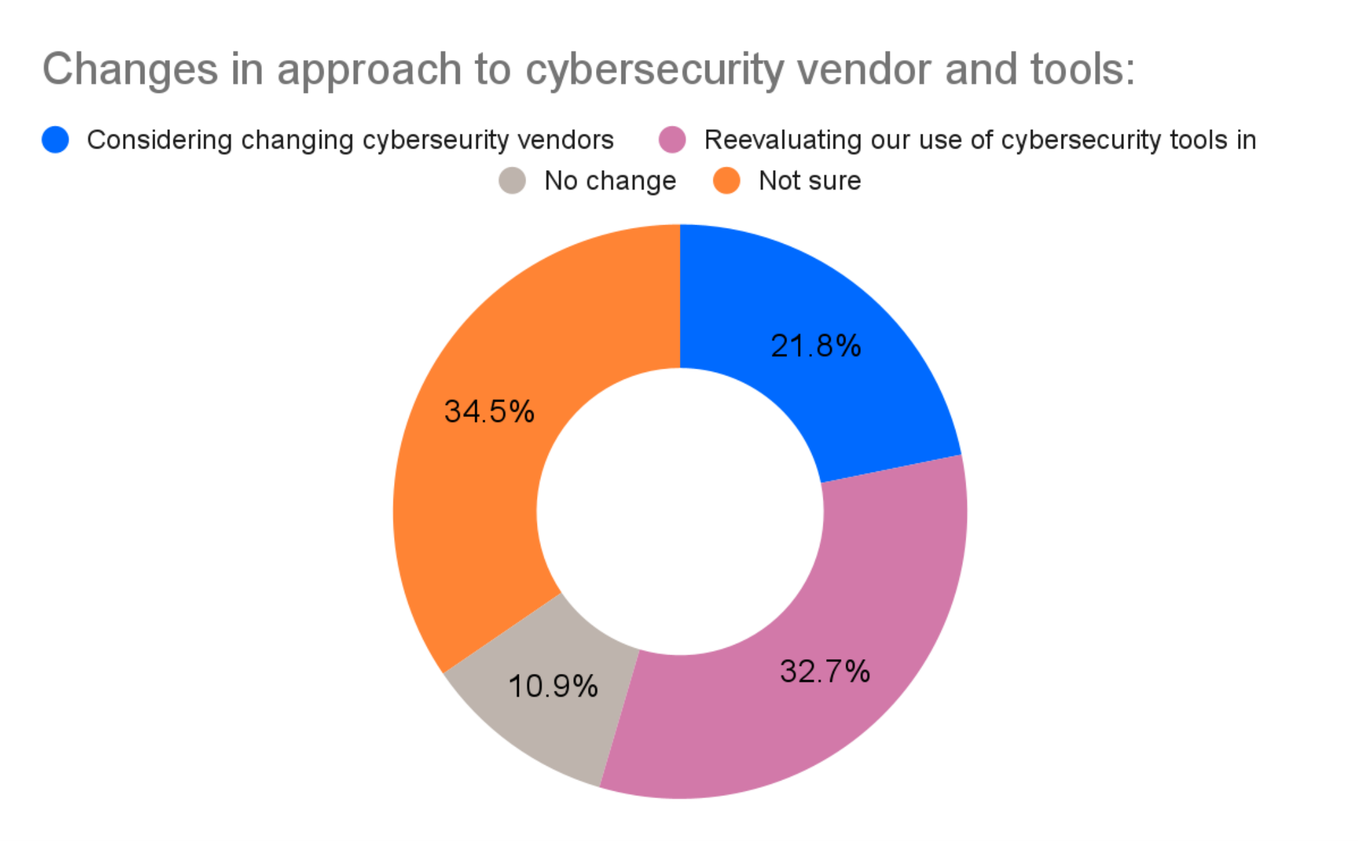
86 % Ja

92 % Technologie
70 % Regierung / Öffentlicher Sektor

F20. Hat Ihr Unternehmen als Reaktion auf jüngere Sicherheitsvorfälle wie der Crowdstrike Ausfall seine Vorgehensweise beim Testen oder der Einführung von Updates oder Patches geändert? Bitte eine Antwort auswählen I Basis: 1.800

Umgang mit Cybersicherheitsanbietern und -Tools

Fast die Hälfte (48 %) überdenkt nach dem jüngsten Crowdstrike Ausfall die Nutzung von Cybersicherheitstools im Allgemeinen, und weitere **29 % erwägen einen Anbieterwechsel**.



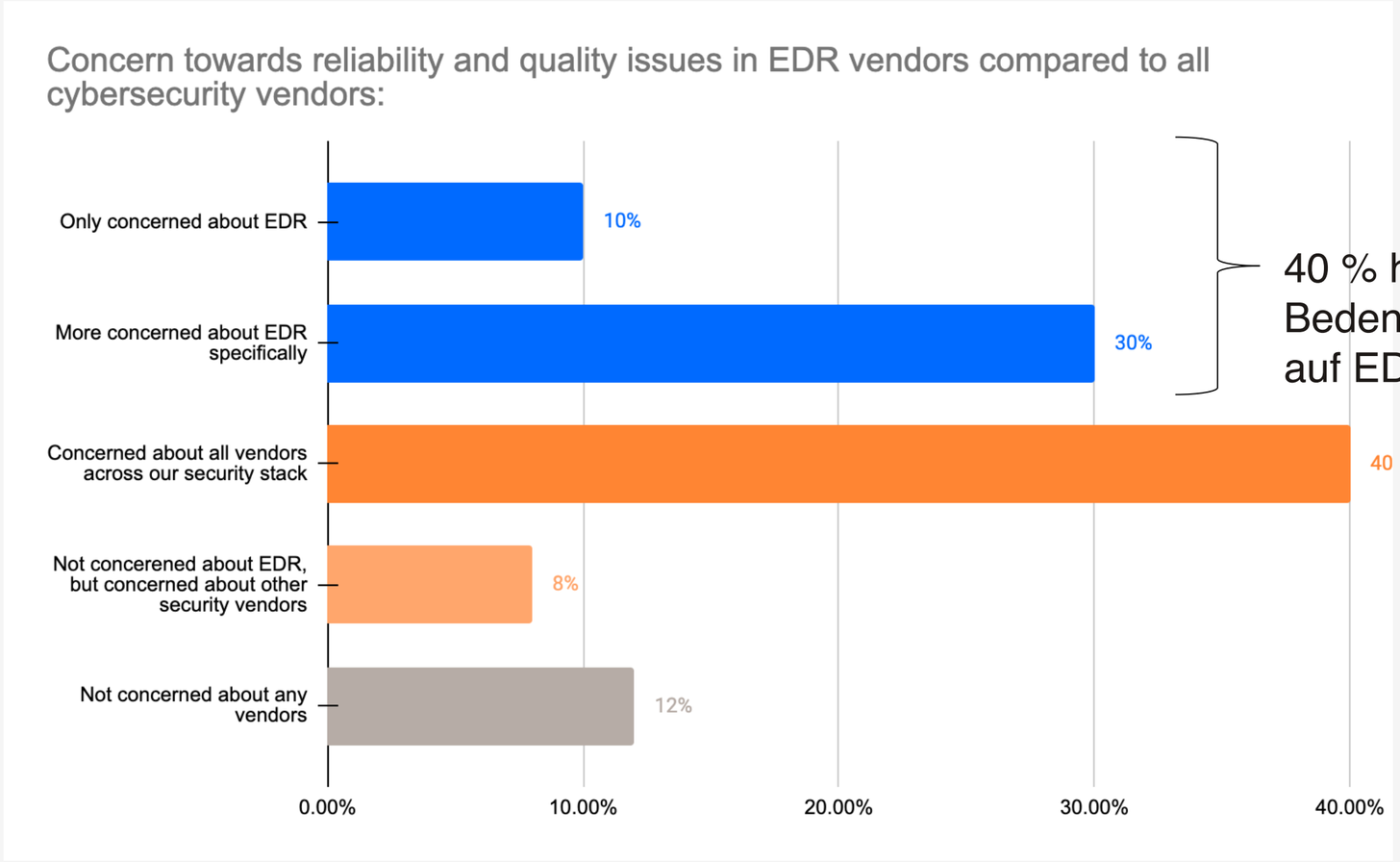
Nach dem Crowdstrike Ausfall sind Unternehmen vorsichtiger geworden, wenn es um Anbieter von Cybersicherheitslösungen und –Tools geht.

Der Ausfall hat zu einer weit verbreiteten Besorgnis geführt, die Unternehmen dazu veranlasst hat, ihre Sicherheitsoptionen zu überdenken.

F21. Hat Ihr Unternehmen als Reaktion auf jüngere Sicherheitsvorfälle wie der Crowdstrike Ausfall seine Vorgehensweise in Bezug auf Cybersicherheitsanbieter und -Tools geändert? Bitte eine Antwort auswählen I Basis: 1.800

Bedenken hinsichtlich der Zuverlässigkeit von EDR-Anbietern

88 % sind besorgt über die Zuverlässigkeit und Qualität ihrer Anbieter, wobei manche Befragten **Bedenken in Bezug auf alle Anbieter in ihrem Sicherheitsstack haben (40 %)** und manche nur **in Bezug auf EDR-Anbieter (40 %)**.



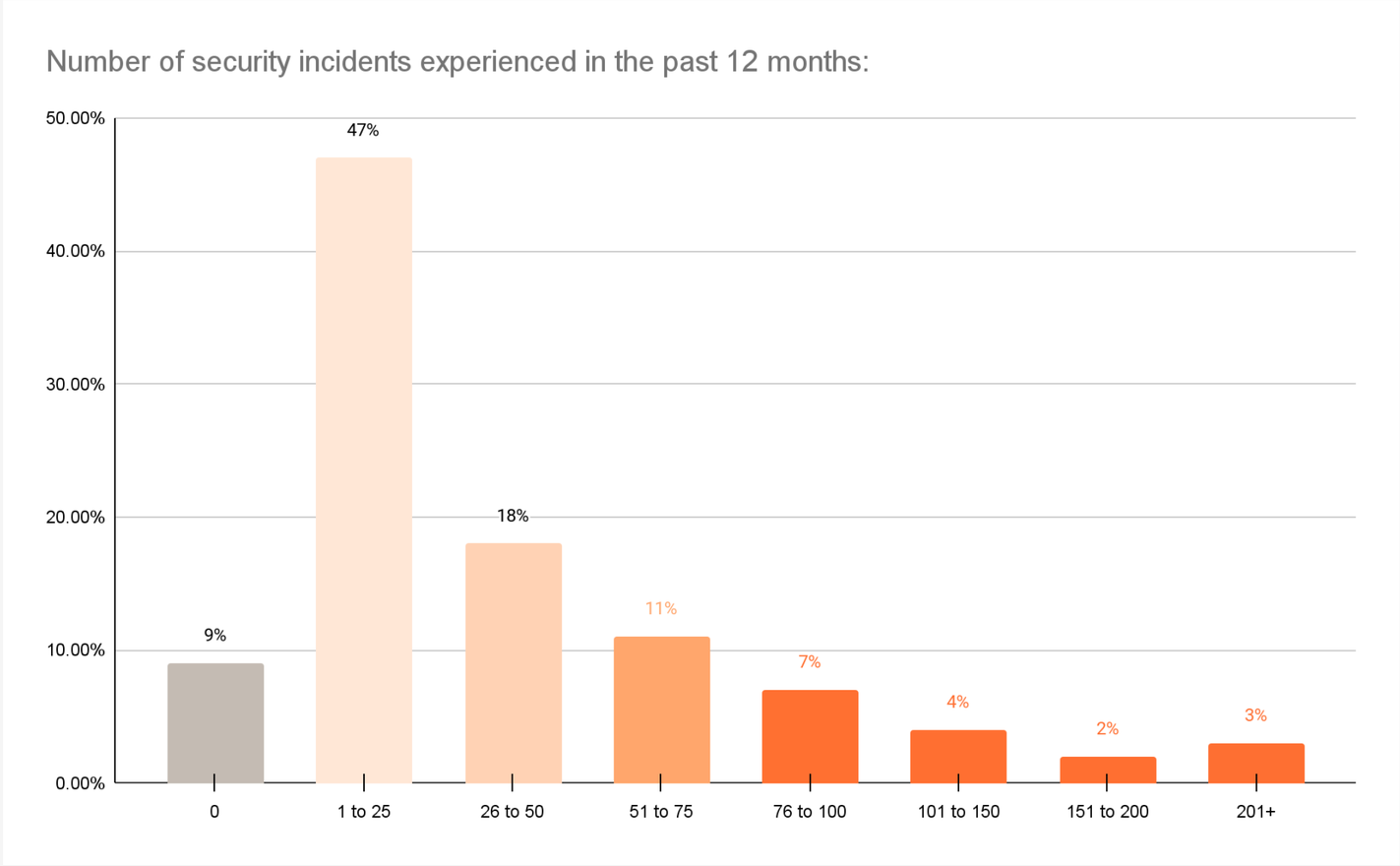
F22a. Inwiefern sind Sie angesichts des Crowdstrike Ausfalls besorgt über die Zuverlässigkeit und Softwarequalität von EDR-Anbietern im Vergleich zu anderen Anbietern von Cybersicherheitsprodukten? Bitte eine Antwort auswählen I Basis: 1.800

Wichtigste Ergebnisse

Die Bedrohungslage

Anzahl der Sicherheitsvorfälle im vergangenen Jahr

Unternehmen waren in den vergangenen 12 Monaten im Durchschnitt von **40 Sicherheitsvorfällen** betroffen, im Bereich Finanzen / Buchhaltung sogar von 47 Sicherheitsvorfällen.



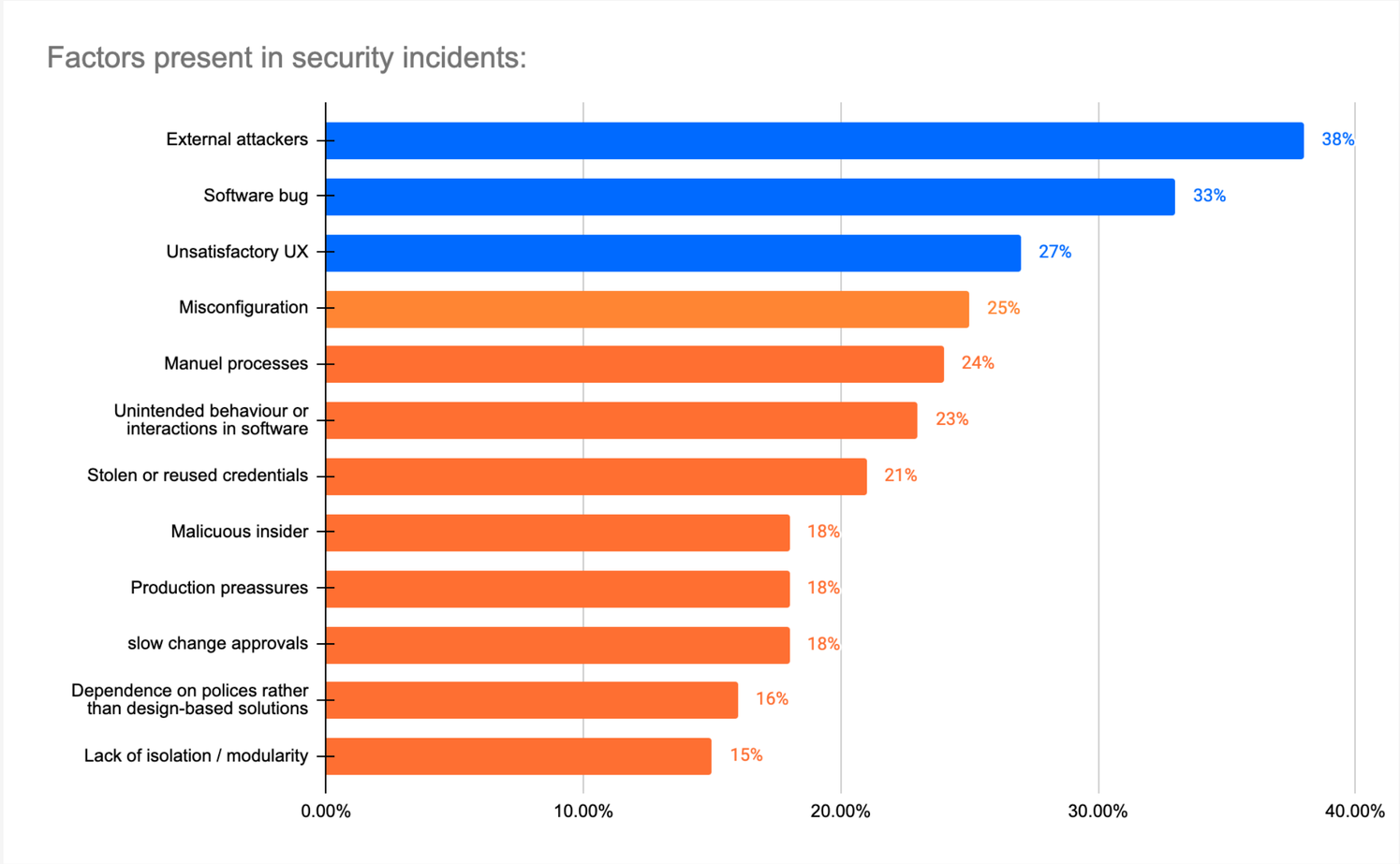
Branche	Durchschnitt
Finanzen / Buchhaltung	47
Regierung / Öffentlicher Sektor	42
Technologie	41
Medien / Unterhaltung / Reisen und Tourismus	36
Groß- und Einzelhandel	33
Gesundheit / Life Sciences	29

Durchschnitt: 40

F15. Von wie vielen Sicherheitsvorfällen, einschließlich solcher, die durch menschliches Versagen verursacht wurden, war Ihr Unternehmen in den letzten 12 Monaten betroffen? Bitte eine Antwort auswählen I Basis: 1.800

Faktoren, die bei Sicherheitsvorfällen eine Rolle spielen

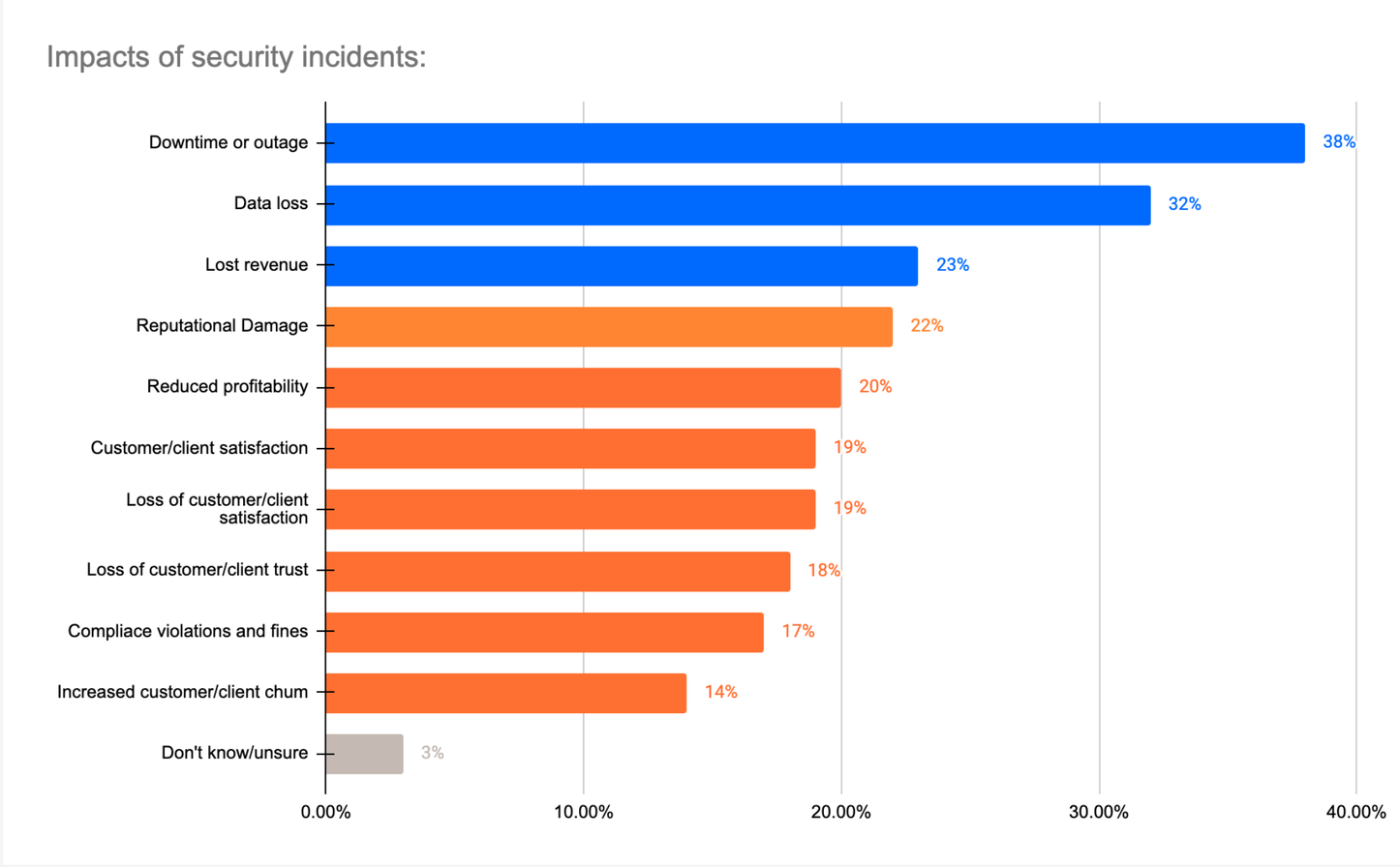
Zu den wichtigsten Faktoren für Sicherheitsverletzungen gehörten **externe Angreifer (38%), Softwarefehler (33%) und ein mangelhaftes Nutzererlebnis (27%)**.



F16. Welche der folgenden Faktoren spielten bei dem Sicherheitsvorfall eine Rolle? Bitte alle zutreffenden Antworten auswählen I Basis: 1.632 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Hauptfolgen von Sicherheitsvorfällen

Zu den Hauptfolgen von Sicherheitsvorfällen gehören **Ausfallzeiten (38 %), Datenverluste (32 %) und Umsatzeinbußen (23 %).**



F17a. Was waren die Hauptfolgen des Sicherheitsvorfalls? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.632 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Hauptfolgen von Sicherheitsvorfällen – nach Branche

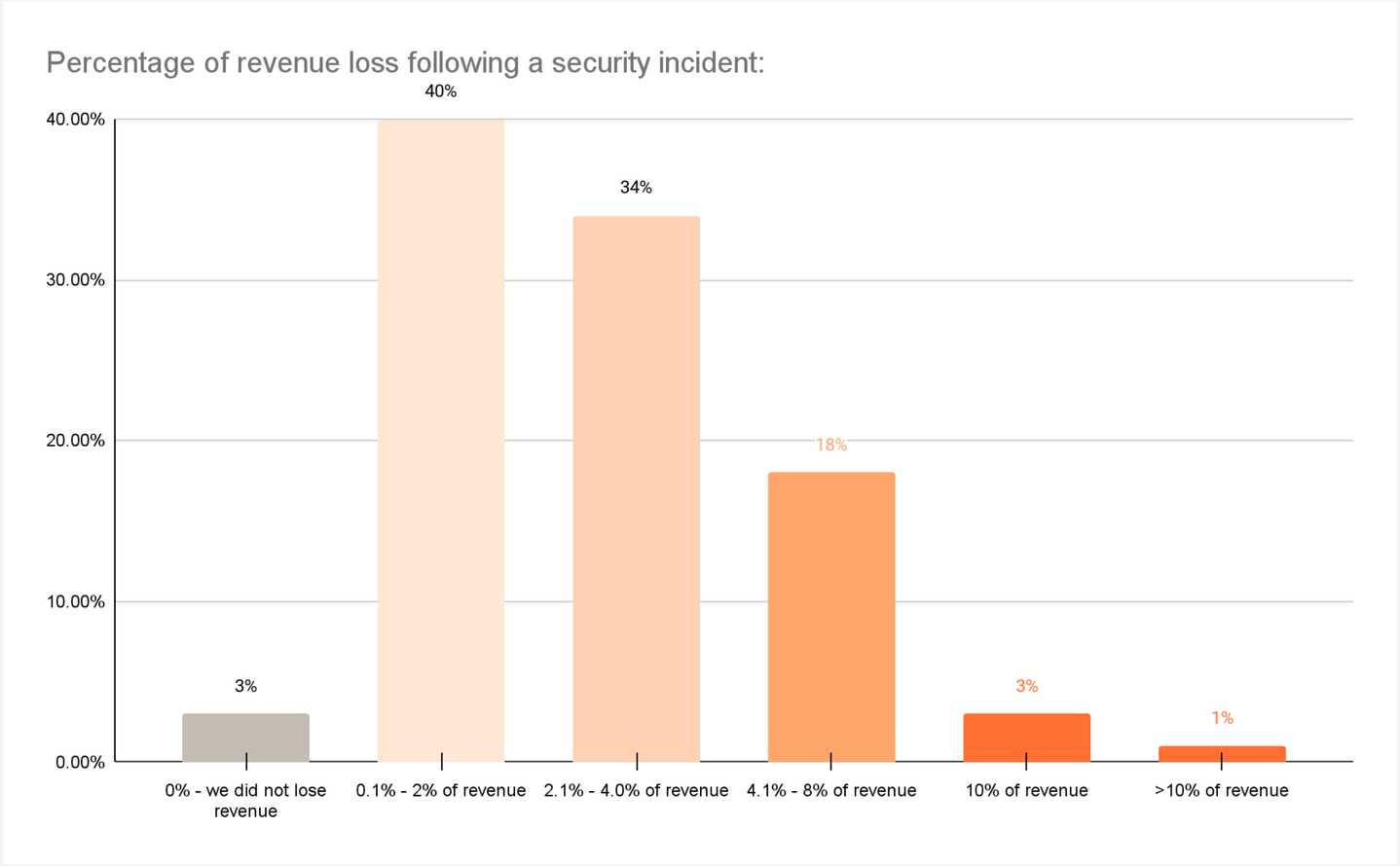
Am stärksten zu spüren waren die Auswirkungen von **Ausfallzeiten** nach Sicherheitsvorfällen im Bereich **Regierung / Öffentlicher Sektor (47 %)**. In der **Technologiebranche** waren es nur **33 %**. Hauptfolgen von Sicherheitsvorfällen nach Branche:

	Finanzen / Buchhaltung	Regierung / Öffentlicher Sektor	Gesundheit / Life Sciences	Medien / Unterhaltung / Reisen und Tourismus	Groß- und Einzelhandel	Technologie
Ausfallzeiten	**39 %**	**47 %**	**38 %**	**42 %**	**42 %**	**33 %**
Datenverlust	**28 %**	**35 %**	**39 %**	**42 %**	**24 %**	**32 %**
Umsatzverlust	**24 %**	**11 %**	**25 %**	**27 %**	**23 %**	**25 %**
Rufschädigung	**23 %**	**26 %**	**18 %**	**16 %**	**27 %**	**25 %**
Geschmälerter Gewinn	**23 %**	**14 %**	**16 %**	**20 %**	**25 %**	**23 %**
Kompromittierte Kundenkonten	**17 %**	**17 %**	**19 %**	**22 %**	**17 %**	**22 %**
Verringerung der Kundenzufriedenheit	**23 %**	**14 %**	**17 %**	**19 %**	**18 %**	**24 %**
Verlust des Kundenvertrauens	**19 %**	**13 %**	**18 %**	**20 %**	**19 %**	**17 %**
Compliance-Verstöße und Bußgelder	**21 %**	**14 %**	**18 %**	**18 %**	**16 %**	**16 %**
Erhöhte Kundenabwanderung	**16 %**	**5 %**	**11 %**	**11 %**	**15 %**	**17 %**
Sonstige	**1 %**	**1 %**	**-**	**-**	**-**	**-**
Weiß nicht / Nicht sicher	**2 %**	**7 %**	**3 %**	**1 %**	**3 %**	**2 %**

F17a. Was waren die Hauptfolgen des Sicherheitsvorfalls? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.632

Umsatzeinbußen aufgrund von Sicherheitsvorfällen

Diejenigen Befragten, die Umsatzeinbußen als Hauptfolge von Sicherheitsvorfällen angeben, berichten von einem durchschnittlichen Umsatzverlust von **2,9 %.**



Unternehmensgröße	Durchschnitt
250-999	2,7
1.000-4.999	3,0
5.000-24.999	3,1
>25.000	3,2

Zunehmende Umsatzeinbußen mit der Unternehmensgröße

F17b. Wie viel Prozent Ihres Umsatzes mussten Sie aufgrund eines Sicherheitsvorfalls ungefähr einbüßen? Bitte eine Antwort auswählen I Basis: 374 * Es wurden nur diejenigen Unternehmen befragt, die in Folge eines Sicherheitsvorfalls Umsätze einbüßen mussten.

Externe Unterstützung bei der Erholung von Sicherheitsvorfällen – nach Branche

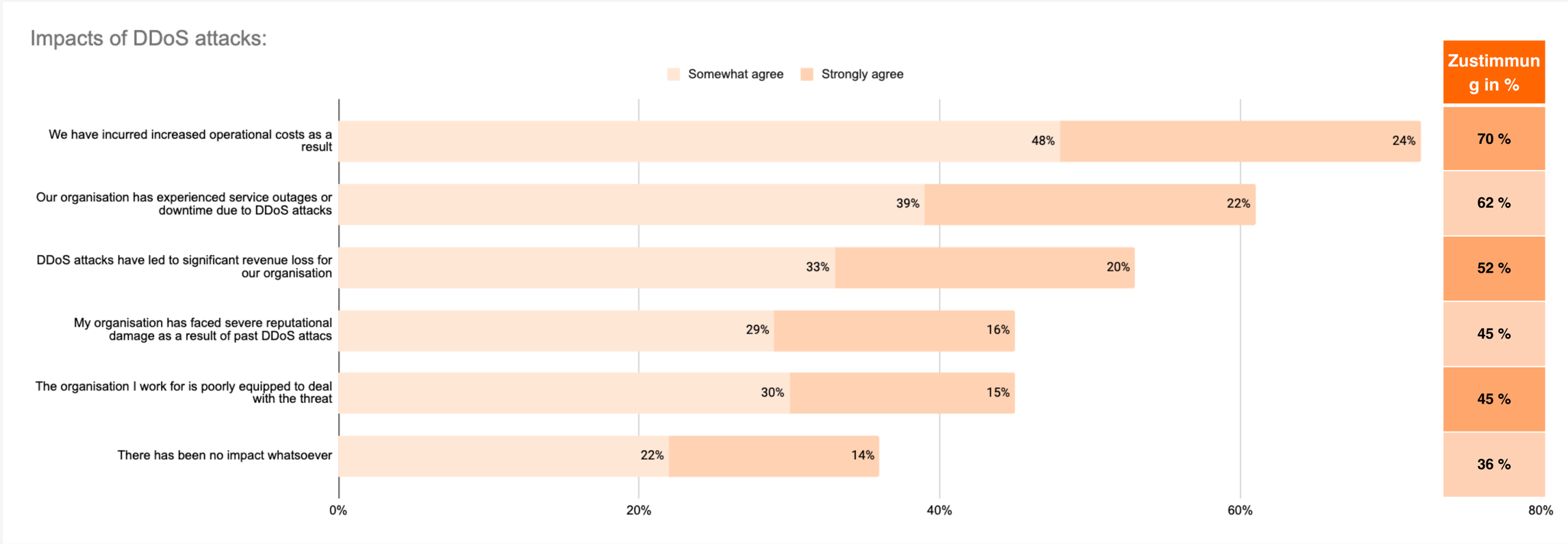
Im Vergleich zu allen anderen Branchen erhielt der Bereich Regierung / Öffentlicher Sektor sehr unterschiedliche externe Unterstützung bei der Erholung von Sicherheitsvorfällen. Externe Unterstützung bei der Erholung von Sicherheitsvorfällen nach Branche:

	Finanzen / Buchhaltung	Regierung / Öffentlicher Sektor	Gesundheit / Life Sciences	Medien und Unterhaltung / Reisegewerbe und Tourismus	Groß- und Einzelhandel	Technologie
Cybersicherheitsberater	**53 %**	**35 %**	**47 %**	**56 %**	**57 %**	**57 %**
Anbietersupport	**37 %**	**15 %**	**26 %**	**39 %**	**41 %**	**42 %**
Rechtsberatung	**25 %**	**14 %**	**36 %**	**30 %**	**26 %**	**25 %**
PR- und Krisenmanagementunternehmen	**27 %**	**12 %**	**29 %**	**26 %**	**22 %**	**31 %**
Branchenverbände	**19 %**	**16 %**	**19 %**	**18 %**	**27 %**	**29 %**
Regierungsbehörden	**21 %**	**45 %**	**21 %**	**17 %**	**14 %**	**23 %**
Sonstige	**1 %**	**-**	**0 %**	**-**	**-**	**-**
Unser Unternehmen hat bei der Erholung von Sicherheitsvorfällen keine externe Unterstützung erhalten.	**12 %**	**18 %**	**13 %**	**9 %**	**13 %**	**6 %**

F22a: Welche externe Unterstützung oder H
zutreffenden Antworten auswählen | Basis: 1.

Auswirkungen von DDoS-Angriffen

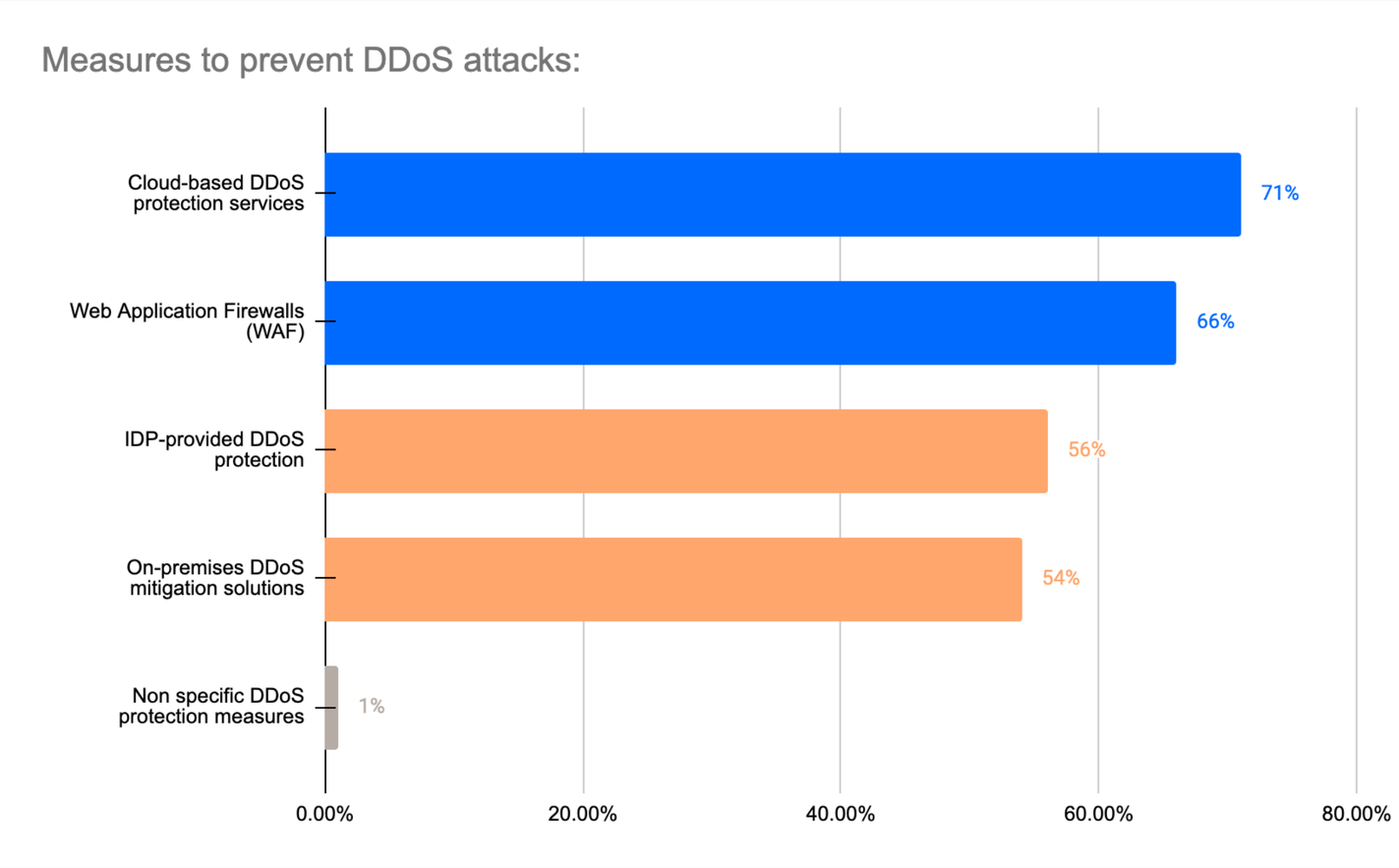
Entscheider, die glauben, dass DDoS-Angriffe in den nächsten 12 Monaten zu den größten Bedrohungen gehören werden, lassen sich voraussichtlich von den erheblichen negativen Auswirkungen von DDoS-Angriffen leiten: **70 %** sagen, dass diese zu **erhöhten Betriebskosten** führen.



F1b. Inwiefern stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 421 * Es wurden nur diejenigen befragt, die glauben, dass DDoS-Angriffe eine Bedrohung darstellen.

DDoS-Schutzmaßnahmen

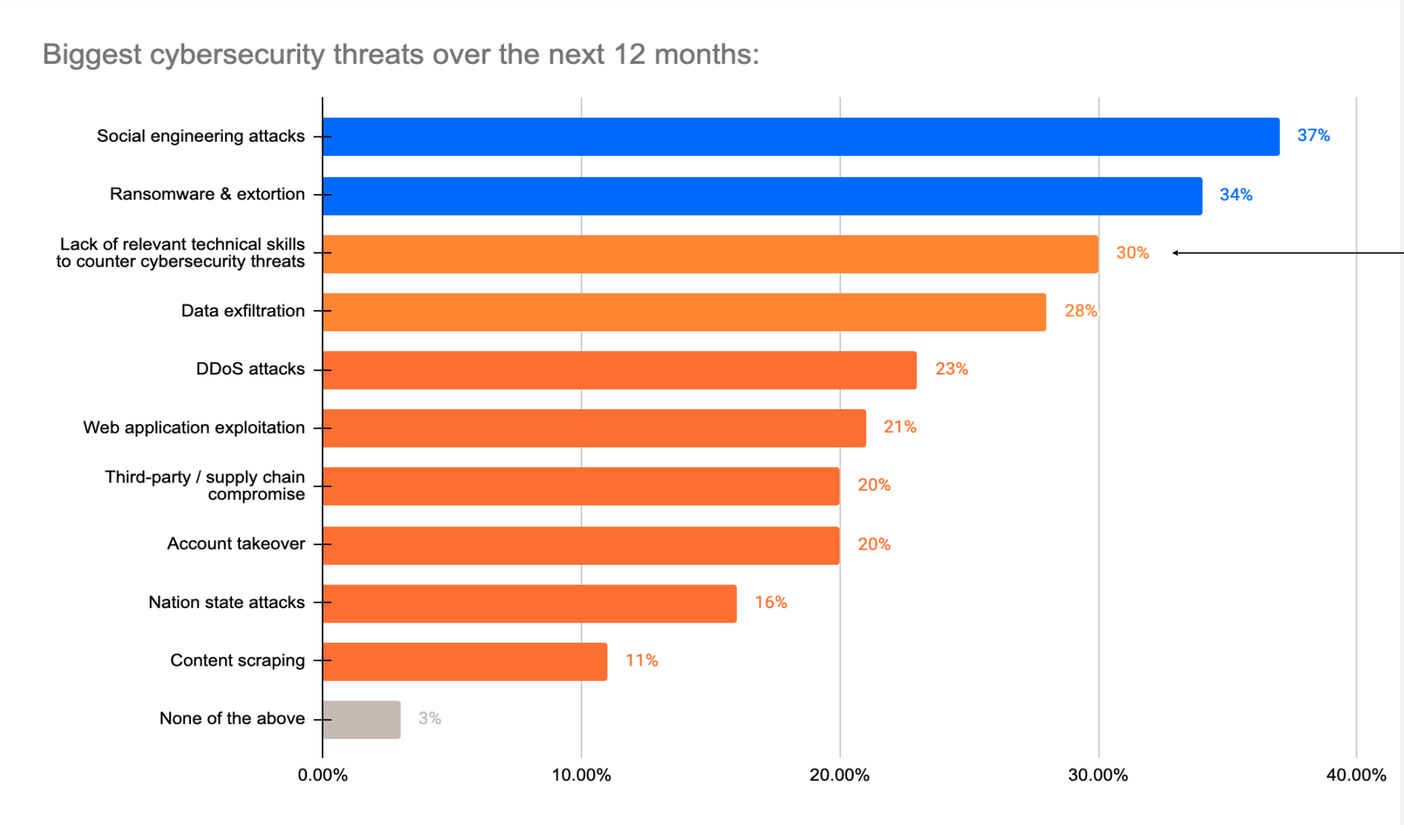
Unternehmen nutzen am häufigsten **cloudbasierte DDoS-Schutzservices (71 %)** und **WAFs (66 %)** zur Bekämpfung von DDoS-Angriffen.



F1c. Welche Maßnahmen setzt Ihr Unternehmen derzeit zum Schutz vor DDoS-Angriffen ein? Bitte alle zutreffenden Antworten auswählen I Basis: 421 * Es wurden nur diejenigen befragt, die glauben, dass DDoS-Angriffe eine Bedrohung darstellen.

Größte prognostizierte Bedrohungen für die Cybersicherheit

Unternehmen gehen davon aus, dass **Social-Engineering-Angriffe (37 %)** sowie **Ransomware und Erpressung (34 %)**, dicht gefolgt von einem **Mangel an relevanten Fachkenntnissen (30 %)** in den nächsten 12 Monaten die größten Bedrohungen für ihre Cybersicherheit darstellen werden.

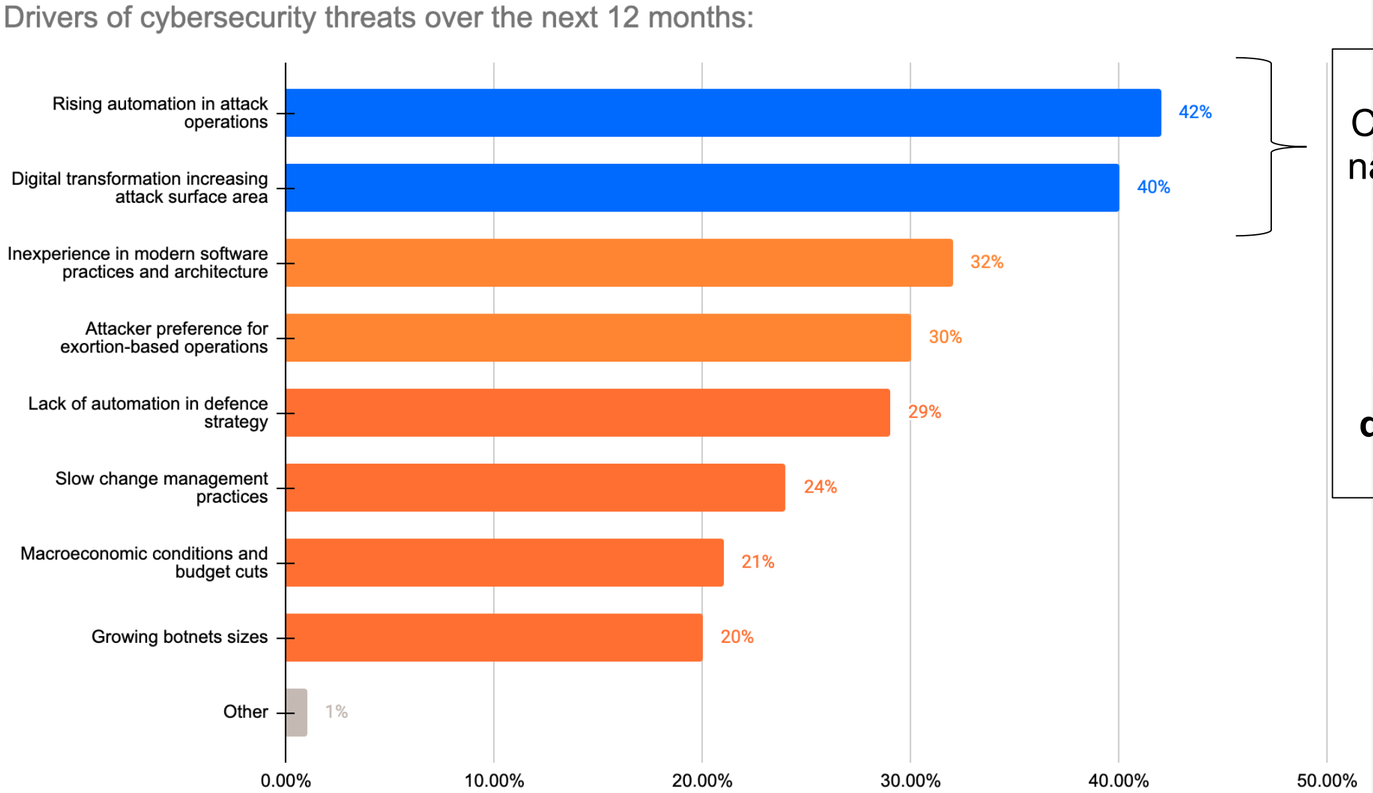


Der Anstieg auf 35 % im Bereich Medien / Unterhaltung / Reisen und Tourismus deutet darauf hin, dass es sich hierbei insbesondere um ein Fachkräfteproblem handelt.

F1a. Was wird Ihrer Meinung nach in den nächsten 12 Monaten die größte Bedrohung für die Cybersicherheit in Ihrem Unternehmen darstellen? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.800

Treibende Kräfte hinter zukünftigen Cybersicherheitsbedrohungen

Mit Blick auf die Zukunft glauben Entscheider, dass die **zunehmende Automatisierung von Angriffen (42 %)** und die **immer größere Angriffsfläche aufgrund der digitalen Transformation (40 %)** die wichtigsten treibenden Kräfte hinter Cybersicherheitsbedrohungen sein werden.



Die wichtigsten Ursachen für Cybersicherheitsbedrohungen in den nächsten 12 Monaten lassen sich auf die Entwicklungen im digitalen Umfeld zurückführen.

Wenn sich Unternehmen weiterentwickeln, ist es wichtig, dass sich die Cybersicherheit mit ihnen weiterentwickelt.

F3. Welche der folgenden Faktoren werden sich Ihrer Meinung nach in den kommenden 12 Monaten auf die Cybersicherheit Ihres Unternehmens auswirken? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.800

Treibende Kräfte hinter zukünftigen Cybersicherheitsbedrohungen – nach Branche

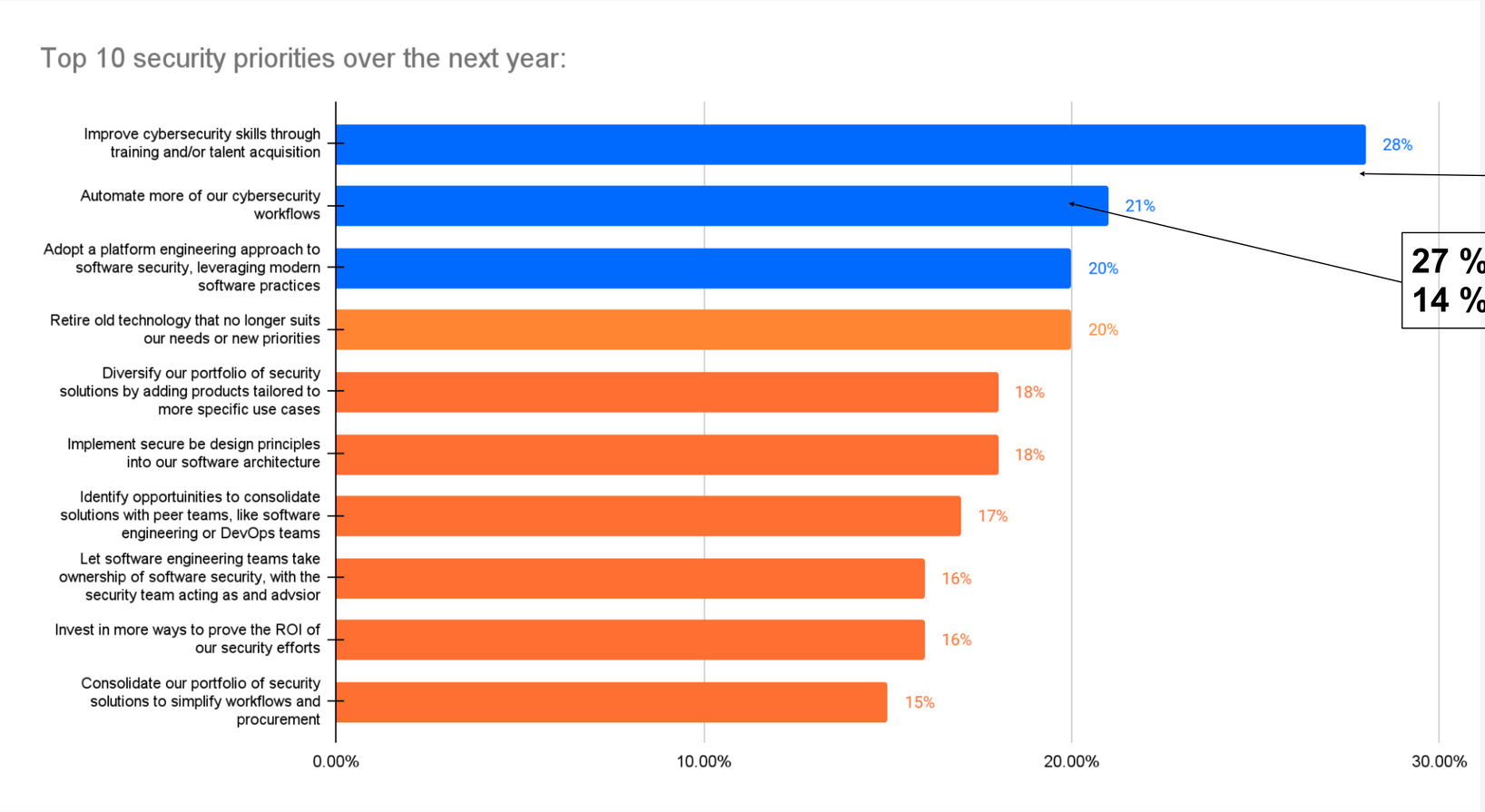
Die **zunehmende Automatisierung von Angriffen** gilt im Bereich **Finanzen / Buchhaltung** als größte Bedrohung **(47 %)**.

	Finanzen / Buchhaltung	Regierung / Öffentlicher Sektor	Gesundheit / Life Sciences	Medien / Unterhaltung / Reisen und Tourismus	Groß- und Einzelhandel	Technologie
Zunehmende Automatisierung von Angriffen	**47 %**	**45 %**	**40 %**	**43 %**	**38 %**	**39 %**
Die digitale Transformation sorgt für eine größere Angriffsfläche	**45 %**	**40 %**	**40 %**	**45 %**	**42 %**	**42 %**
Mangel an Erfahrung mit modernen Softwarepraktiken und -architekturen	**25 %**	**31 %**	**35 %**	**32 %**	**37 %**	**32 %**
Angreifer bevorzugen erpresserische Methoden	**29 %**	**25 %**	**33 %**	**27 %**	**33 %**	**30 %**
Fehlende Automatisierung in der Abwehrstrategie	**27 %**	**26 %**	**23 %**	**35 %**	**24 %**	**35 %**
Langsame Change-Management-Praktiken	**26 %**	**26 %**	**33 %**	**23 %**	**23 %**	**22 %**
Makroökonomische Bedingungen und Budgetkürzungen	**24 %**	**22 %**	**16 %**	**23 %**	**21 %**	**22 %**
Immer größere Botnetze	**24 %**	**20 %**	**17 %**	**21 %**	**19 %**	**22 %**
Sonstige	**0 %**	**1 %**	**0 %**	**-**	**1 %**	**1 %**

F3. Welche der folgenden Faktoren werden sich Ihrer Meinung nach in den kommenden 12 Monaten auf die Cybersicherheit Ihres Unternehmens auswirken? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.800

Sicherheitsprioritäten für das kommende Jahr

Die wichtigsten Sicherheitsprioritäten der Unternehmen für das kommende Jahr betreffen die **Verbesserung ihrer Cybersicherheitskompetenzen (28 %)** und die **Automatisierung von Cybersicherheits-Workflows (21 %)**.



33 % Groß- und Einzelhandel
24 % Technologie

27 % Finanzen / Buchhaltung
14 % Gesundheit / Life Sciences

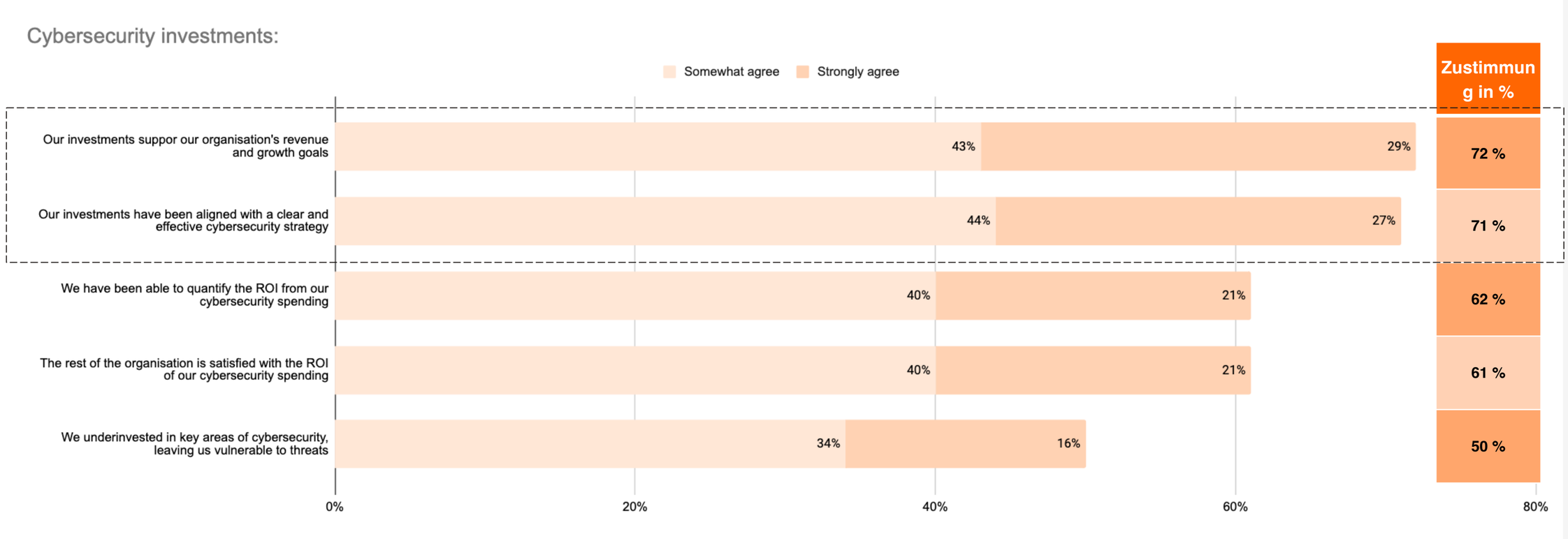
F14. Welche Prioritäten setzt Ihr Unternehmen in puncto Security für das kommende Jahr? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.800

Wichtigste Ergebnisse

Kommen die Ausgaben für die Cybersicherheit zu kurz?

Investitionen in die Cybersicherheit

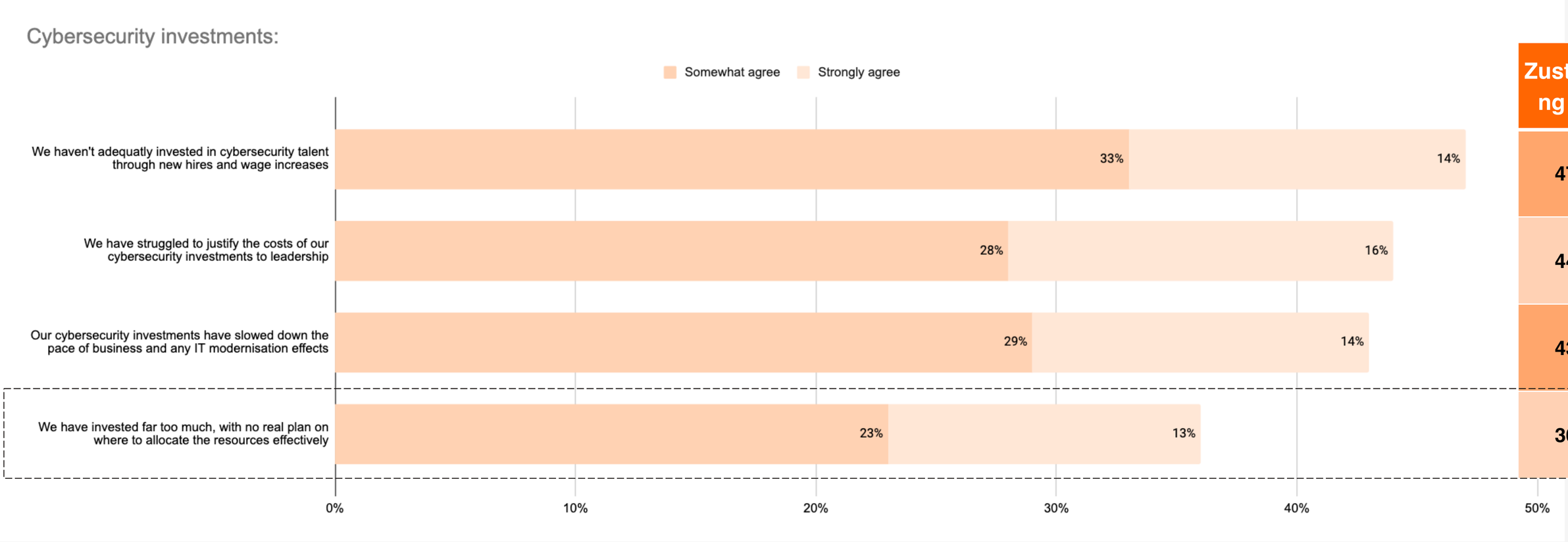
Fast drei Viertel (72 %) sind der Meinung, dass ihre Investitionen in die Cybersicherheit **die Umsatz- und Wachstumsziele ihres Unternehmens unterstützen**, und weitere **71 %** sind der Ansicht, dass diese Investitionen **auf eine klare und effektive Cybersicherheitsstrategie ausgerichtet** sind.



F6j. Denken Sie an die Investitionen, die Sie in den letzten 12 Monaten zur Vorbereitung auf Cybersicherheitsrisiken getätigt haben. Inwiefern stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 1.800

Investitionen in die Cybersicherheit

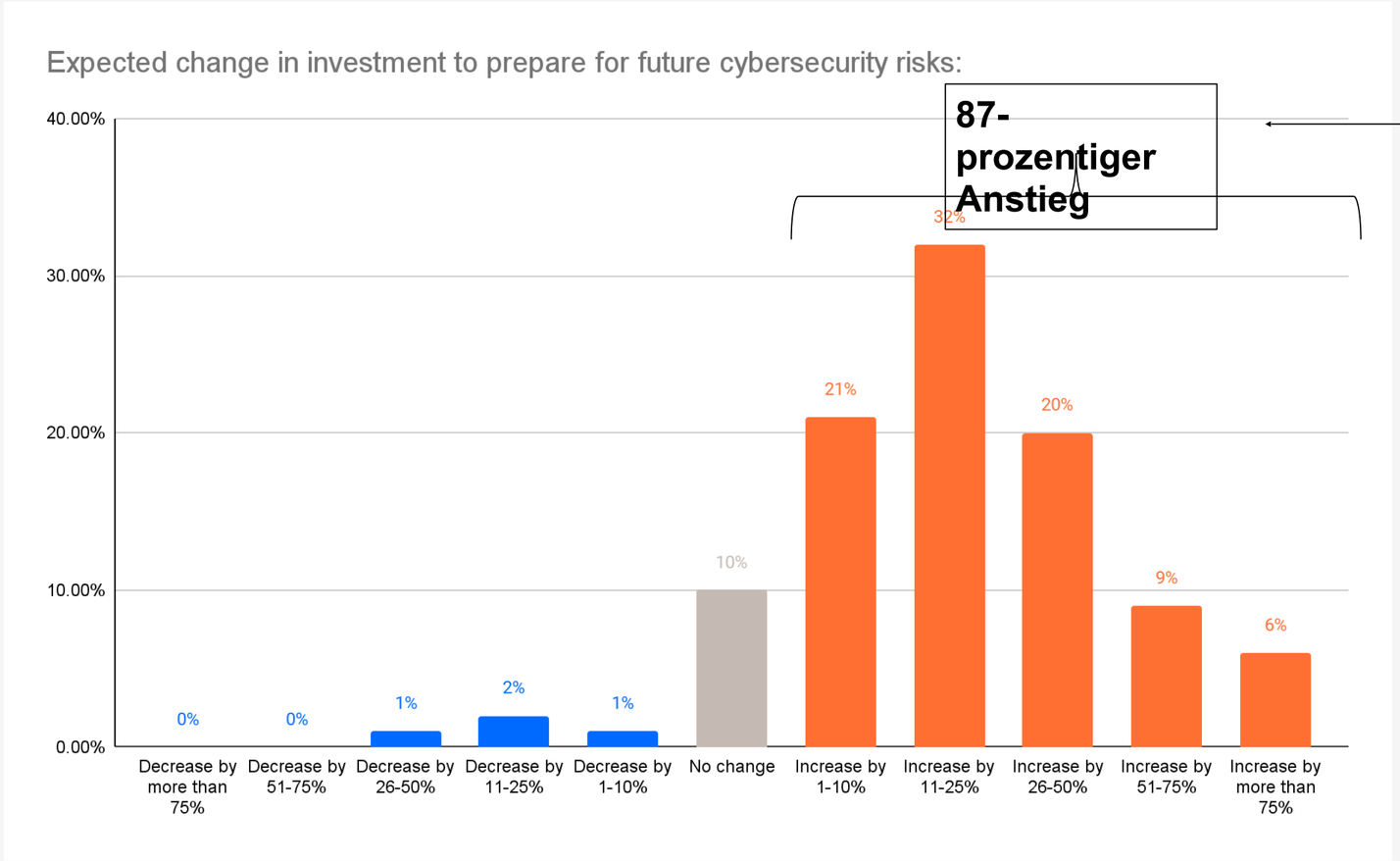
Außerdem stimmen nur **36 %** zu, dass sie **zu viel investiert haben, ohne einen wirklichen Plan zu haben, wie sie die Ressourcen effektiv einsetzen können**. Dies zeigt, dass sich Unternehmen aktiv auf zukünftige Cybersicherheitsrisiken vorbereiten.



F6j. Denken Sie an die Investitionen, die Sie in den letzten 12 Monaten zur Vorbereitung auf Cybersicherheitsrisiken getätigt haben. Inwiefern stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 1.800

Änderungen bei künftigen Investitionen in die Cybersicherheit

87 % der Entscheider erwarten, dass die Investitionen ihres Unternehmens im Hinblick auf die Vorbereitung auf künftige Cybersicherheitsrisiken in den nächsten 12 Monaten **steigen** werden.

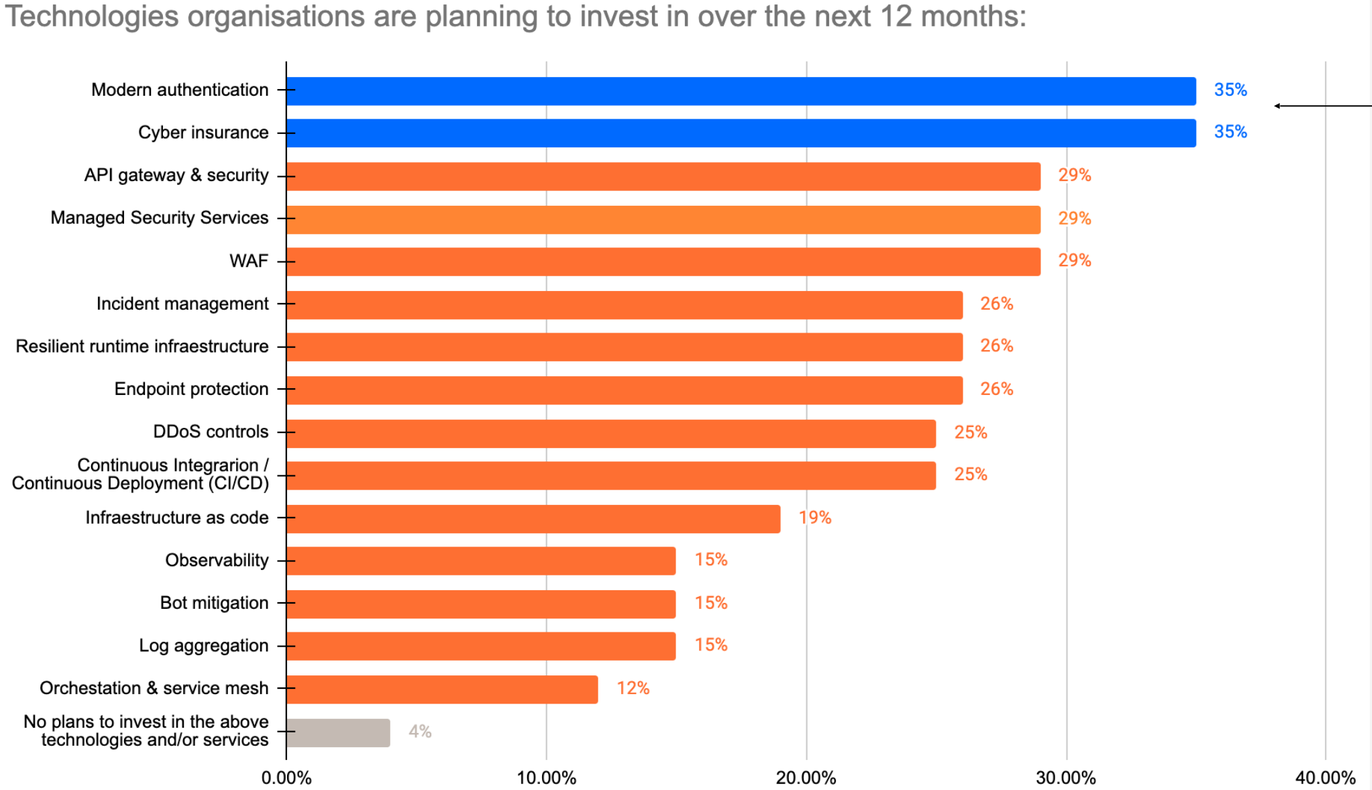


91 % in Finanzen / Buchhaltung, Medien / Unterhaltung / Reisen und Tourismus und Technologie
79 % Regierung / Öffentlicher Sektor

F5. Wie werden sich Ihrer Meinung nach die Investitionen Ihres Unternehmens zur Vorbereitung auf künftige Cybersicherheitsrisiken in den nächsten 12 Monaten verändern? Bitte eine Antwort auswählen I Basis: 1.800

Geplante Investitionen in Cybersicherheitstechnologien

Fast alle Unternehmen planen, in den nächsten 12 Monaten in Technologien zu investieren, insbesondere in **moderne Authentifizierung** und **Cyberversicherungen (je 35 %)**.



44 % Medien / Unterhaltung / Reisen und Tourismus
25 % Regierung / Öffentlicher Sektor

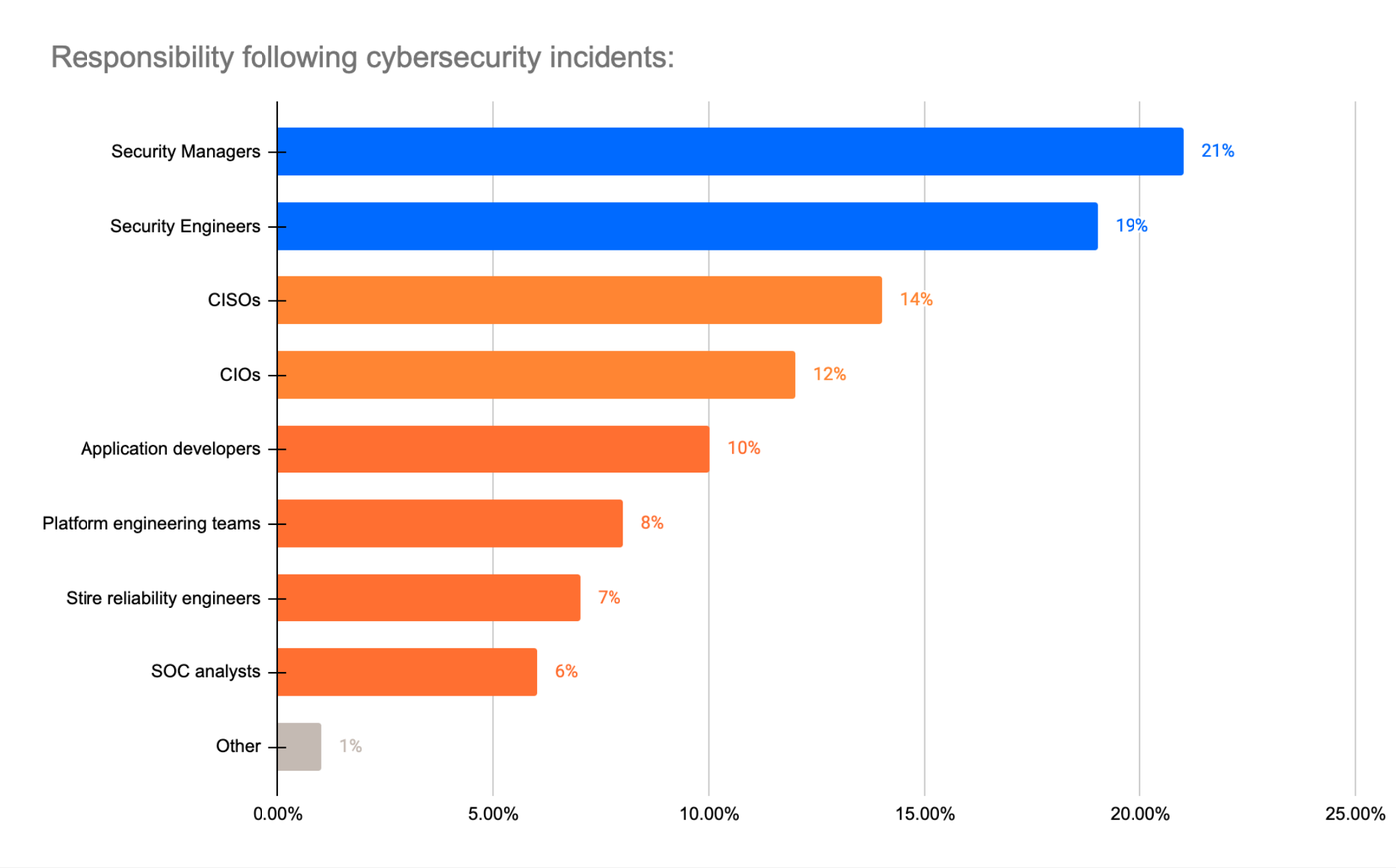
F4. In welche Technologien bzw. Services plant Ihr Unternehmen in den nächsten 12 Monaten zu investieren? Bitte alle zutreffenden Antworten auswählen I Basis: 1.800

Wichtigste Ergebnisse

Verschiebungen der Zuständigkeiten

Verantwortung für Cybersicherheitsvorfälle

Die Personenkreise, die für Sicherheitsvorfälle zur Verantwortung gezogen werden, sind breit gestreut. Am häufigsten tragen allerdings **Security Manager (21 %)** und **Entwickler (19 %)** die Verantwortung für Cybersicherheitsvorfälle.



F9. Wer wird Ihrer Meinung nach am häufigsten für Cybersicherheitsvorfälle in Ihrem Unternehmen zur Verantwortung gezogen? Bitte eine Antwort auswählen I Basis: 1.800

Verantwortung für Cybersicherheitsvorfälle – nach Branche

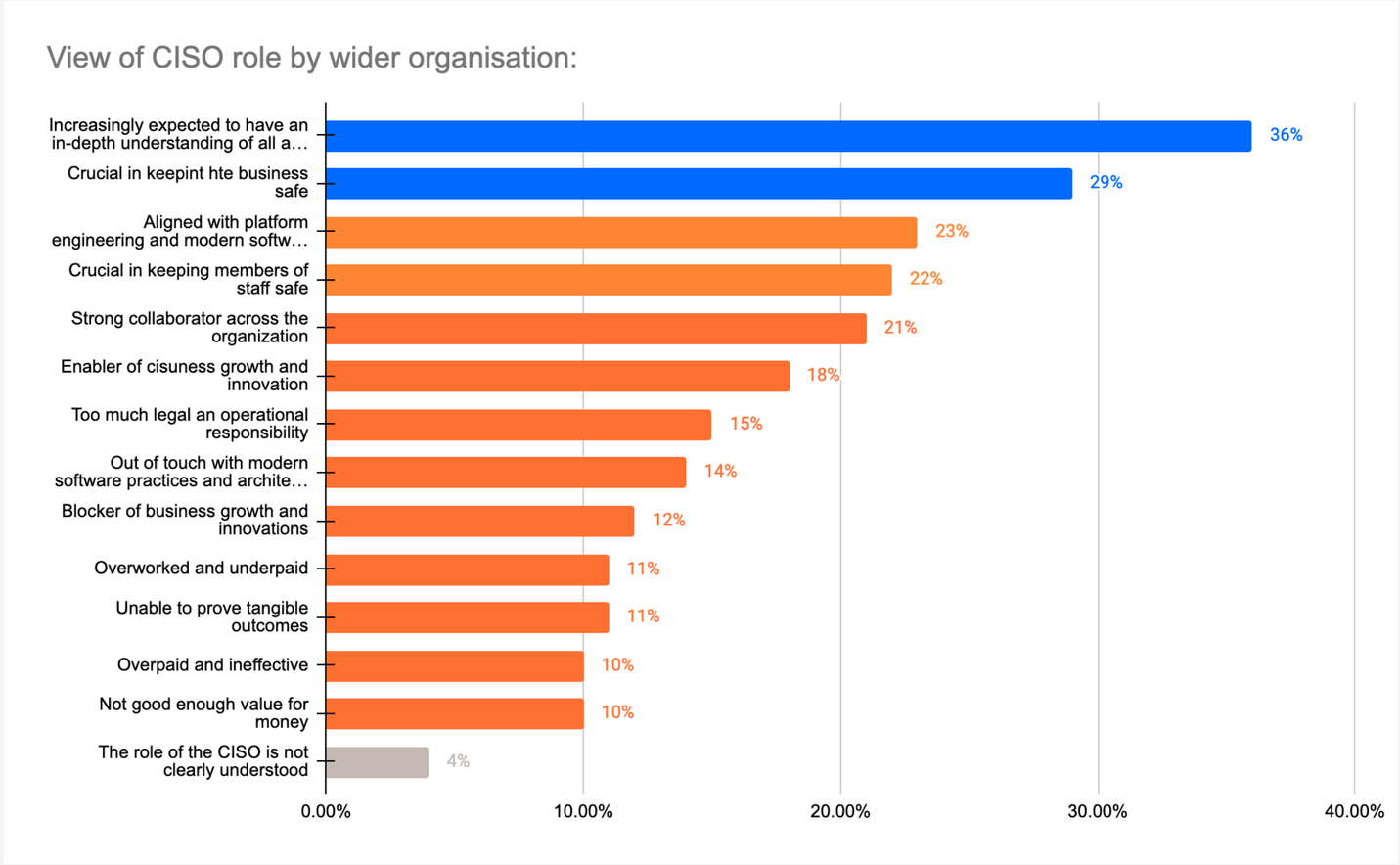
Ein Vergleich der Daten der verschiedenen Branchen zeigt, dass es Unterschiede bei der Zuständigkeit für Cybersicherheitsvorfälle gibt.

	Finanzen / Buchhaltung	Regierung / Öffentlicher Sektor	Gesundheit / Life Sciences	Medien / Unterhaltung / Reisen und Tourismus	Groß- und Einzelhandel	Technologie
Security Manager	**26 %**	**28 %**	**25 %**	**20 %**	**18 %**	**22 %**
Security Engineers	**20 %**	**18 %**	**18 %**	**27 %**	**17 %**	**21 %**
CISOs	**15 %**	**8 %**	**9 %**	**11 %**	**17 %**	**17 %**
CIOs	**11 %**	**15 %**	**13 %**	**8 %**	**14 %**	**11 %**
Anwendungsentwicklung	**9 %**	**9 %**	**11 %**	**12 %**	**10 %**	**10 %**
Platform Engineers	**6 %**	**7 %**	**9 %**	**6 %**	**9 %**	**8 %**
Site Reliability Engineers	**5 %**	**10 %**	**8 %**	**8 %**	**8 %**	**5 %**
SOC-Analysten	**5 %**	**5 %**	**3 %**	**6 %**	**6 %**	**4 %**
Sonstige	**1 %**	**3 %**	**3 %**	**0 %**	**1 %**	**1 %**

F9. Wer wird Ihrer Meinung nach am häufigsten für Cybersicherheitsvorfälle in Ihrem Unternehmen zur Verantwortung gezogen? Bitte eine Antwort auswählen I Basis: 1.800

Wahrnehmung der CISO-Rolle

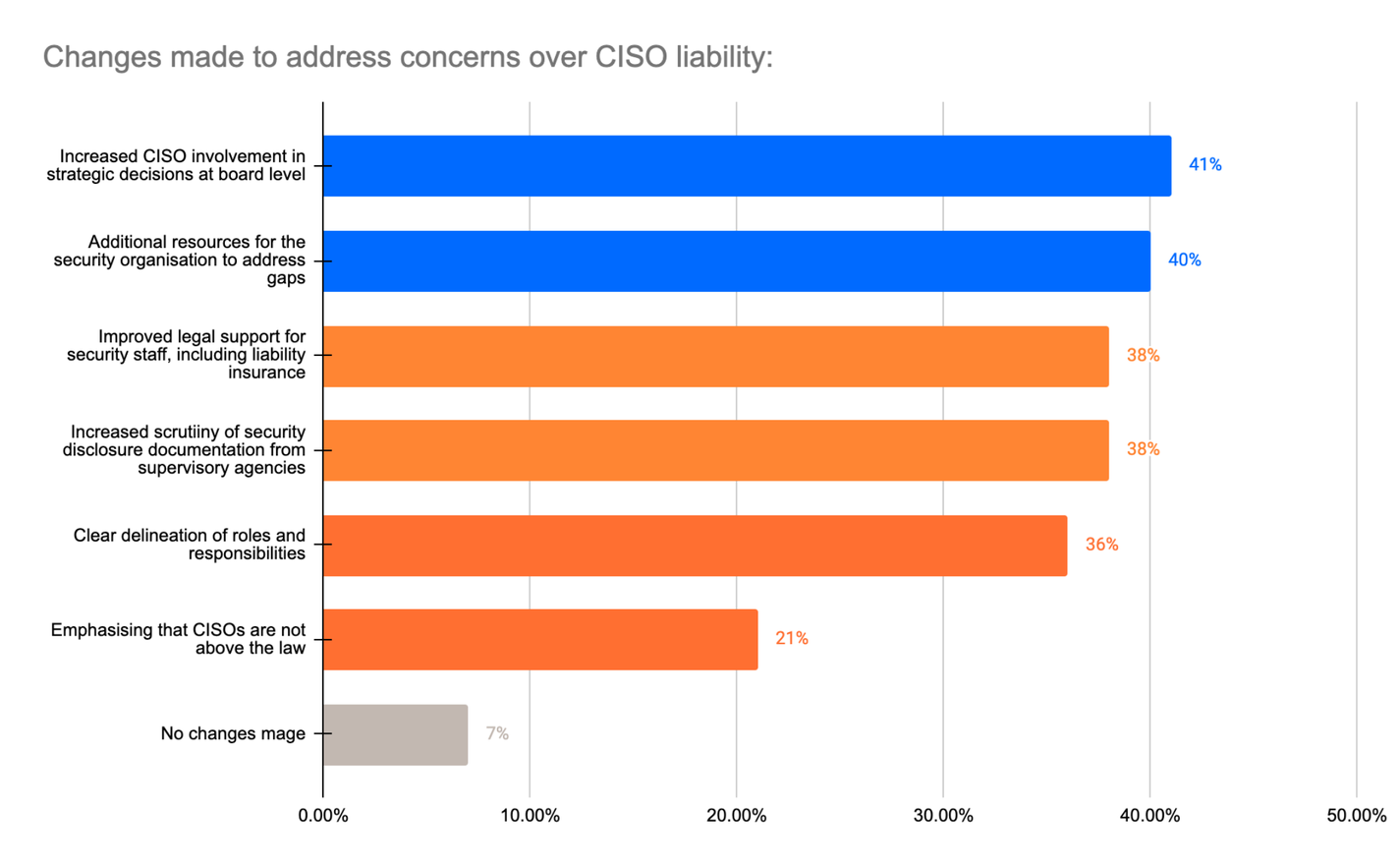
Entscheider sind der Ansicht, dass von CISOs zunehmend erwartet wird, dass sie **über ein tiefgreifendes Verständnis aller IT-Bereiche verfügen (36 %)**, und dass sie **als entscheidend für die Sicherheit des Unternehmens gelten (29 %)**.



F10. Wie wird die Rolle des CISO Ihrer Meinung nach in Ihrem Unternehmen wahrgenommen? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 1.800

Änderungen, die die Verantwortlichkeiten von CISOs betreffen

Unternehmen gehen aktiv gegen Bedenken hinsichtlich der Verantwortlichkeiten von CISOs vor: **41 % beteiligen CISOs stärker an strategischen Entscheidungen** und weitere **40 % schaffen zusätzliche Ressourcen für die Sicherheitsabteilung, um Lücken zu schließen**.

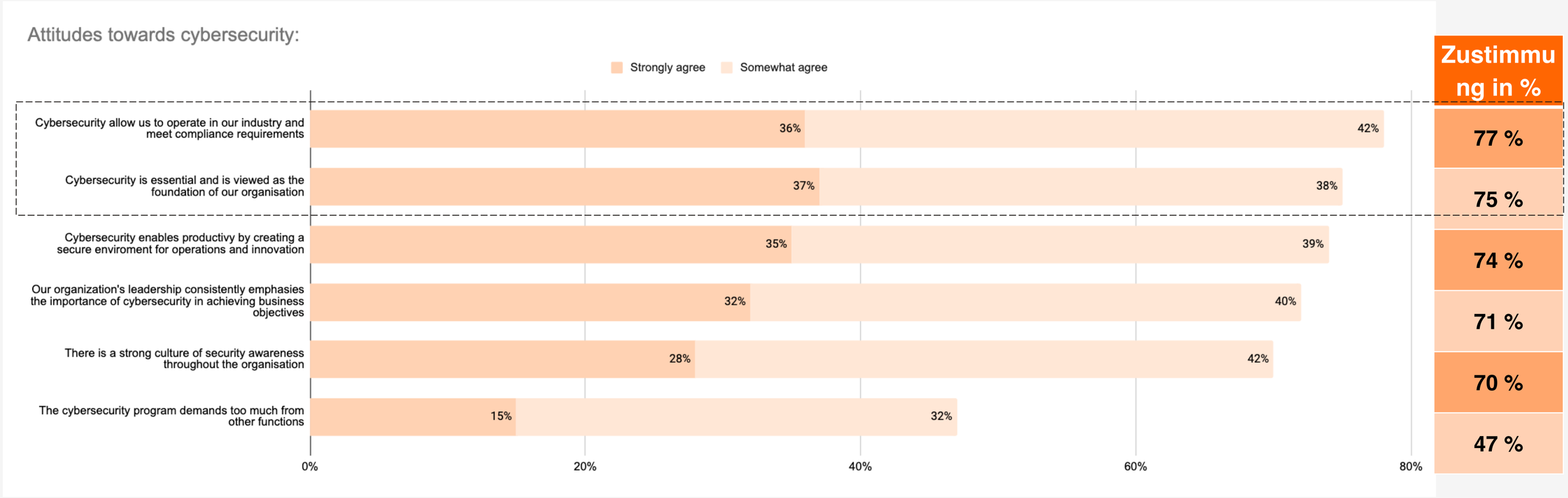


Unternehmen erkennen zunehmend die Bedeutung der Rolle des CISO. Dies deutet auf eine wachsende Anerkennung der strategischen Bedeutung von Cybersicherheit in der Führungsetage hin.

F12. Welche Änderungen hat Ihr Unternehmen hinsichtlich der Verantwortlichkeiten von CISOs bereits umgesetzt? Bitte alle zutreffenden Antworten auswählen I Basis: 1.800

Wahrgenommener Stellenwert von Cybersicherheit

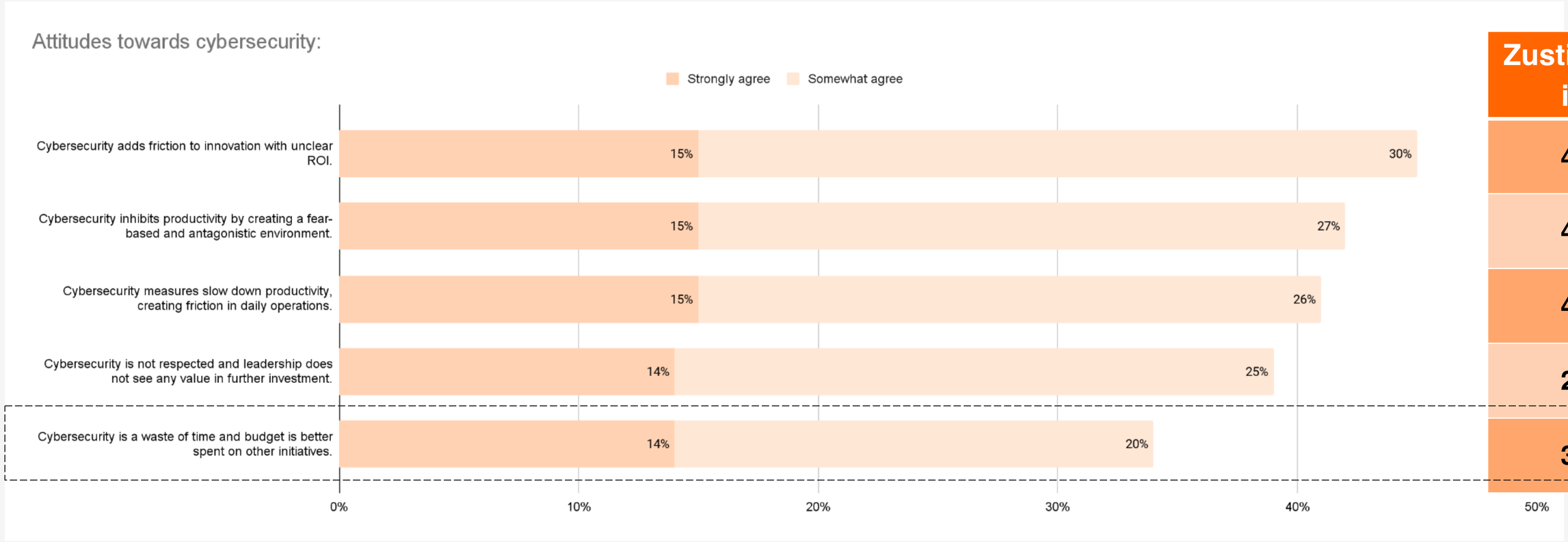
Es herrscht ein starker Konsens darüber, **dass Cybersicherheit unverzichtbar ist (75 %)**, insbesondere **wenn es um die Erfüllung von Compliance-Anforderungen geht (77 %)**.



F11. Denken Sie an den wahrgenommenen Stellenwert der Cybersicherheit in Ihrem Unternehmen. Inwieweit stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 1.800

Wahrgenommener Stellenwert von Cybersicherheit

Nur ein Drittel (34 %) der Befragten sind der Meinung, dass Cybersicherheit eine Zeitverschwendung ist und dass das Budget besser an anderer Stelle eingesetzt werden sollte.

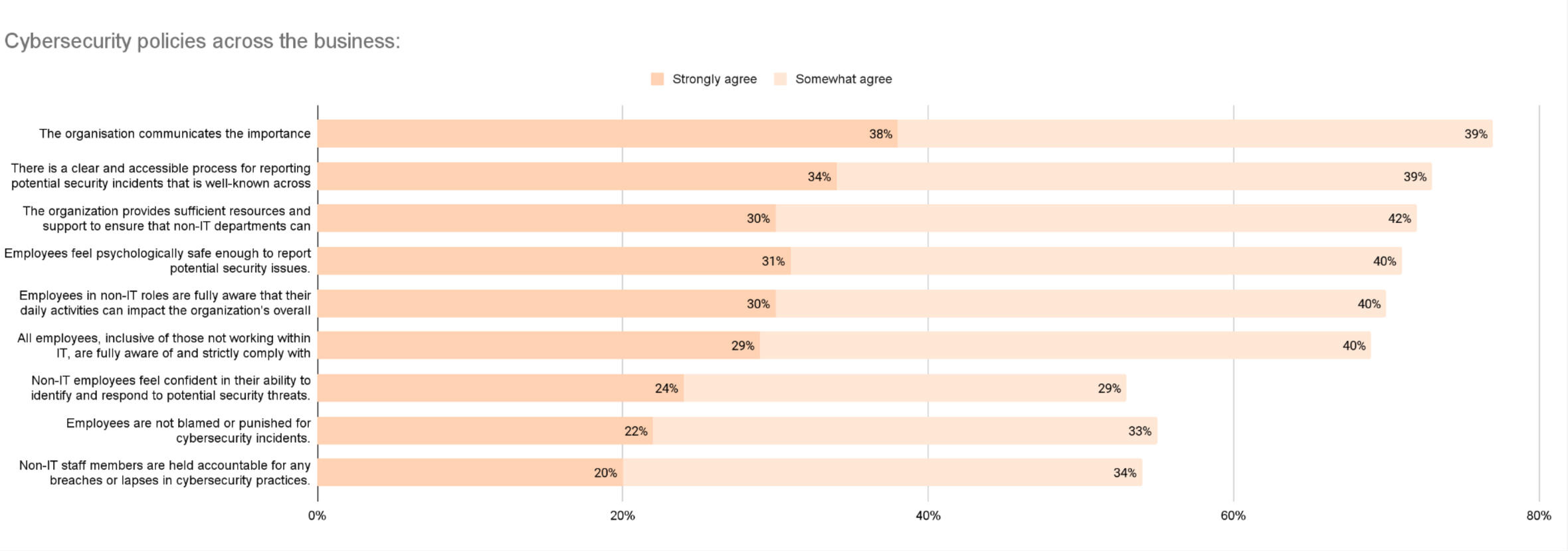


Zustimmung in %
45 %
42 %
42 %
29 %
34 %

F11. Denken Sie an den wahrgenommenen Stellenwert der Cybersicherheit in Ihrem Unternehmen. Inwieweit stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 1.800

Cybersicherheitsrichtlinien

In 2 von 3 Unternehmen herrscht eine ausgeprägte abteilungsübergreifende Compliance-Kultur **(69 %)**, was Richtlinien für die Cybersicherheit betrifft. Diese wird durch eine **effektive Kommunikation über die Bedeutung von Sicherheit (77 %)** unterstützt.



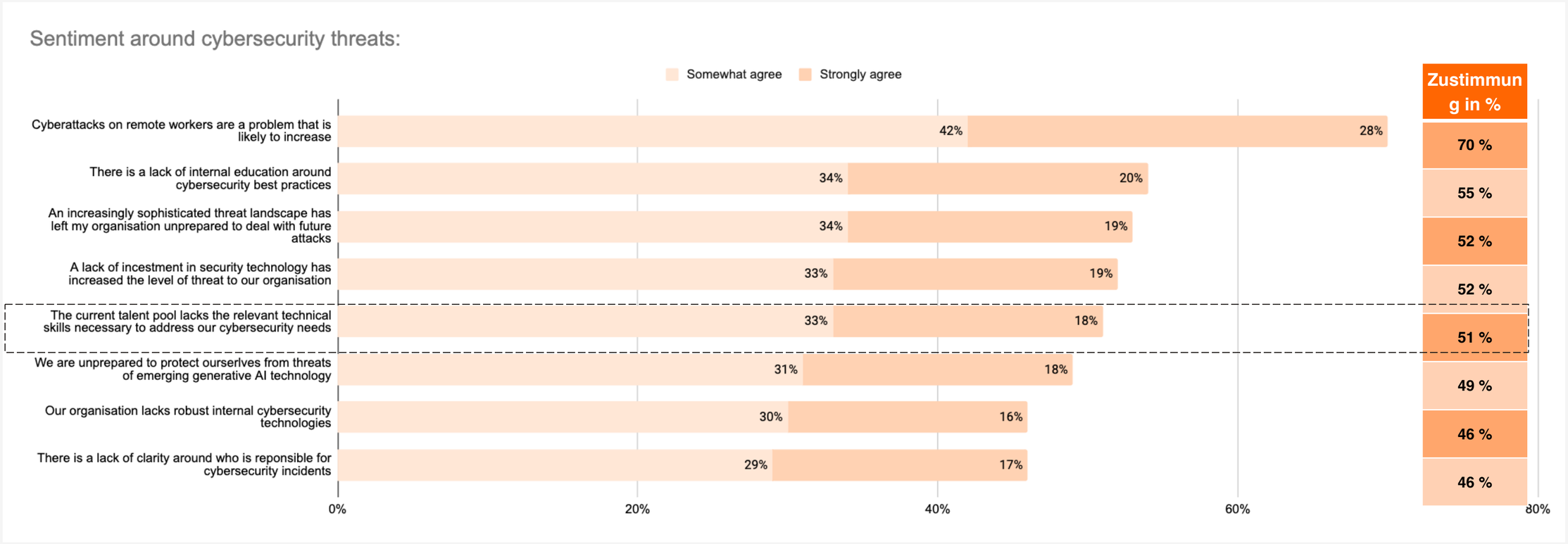
F13. Denken Sie darüber nach, wie gut die Cybersicherheitsrichtlinien in Ihrem Unternehmen von allen Beschäftigten befolgt werden – Nicht-IT-Abteilungen eingeschlossen. Inwieweit stimmen Sie den folgenden Aussagen zu? I Basis: 1.800

Wichtigste Ergebnisse

Talentpool im Bereich Cybersicherheit

Cybersicherheitsrisiken

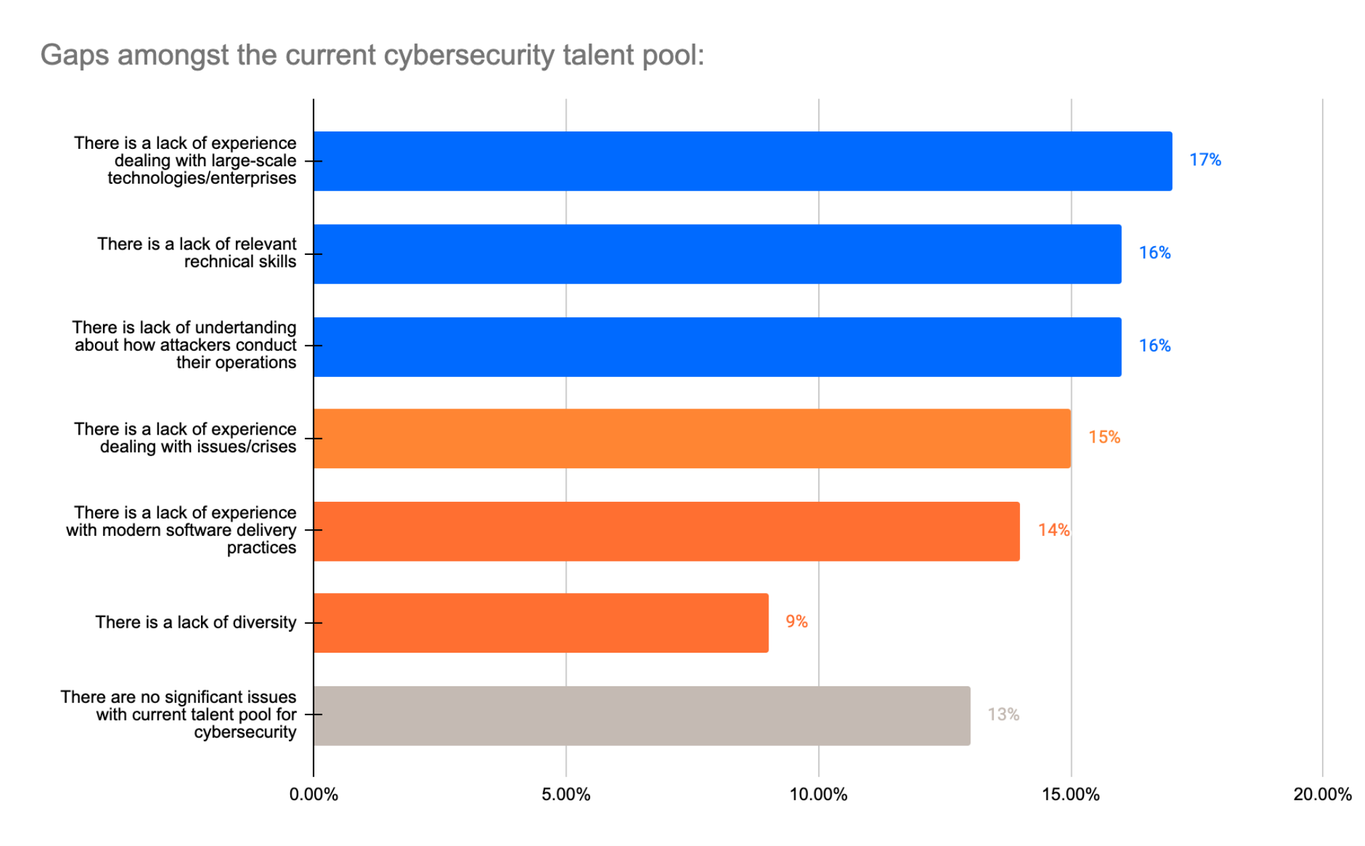
Die Besorgnis über Cyberangriffe auf Remote-Mitarbeiter steigt **(70 %)**, da Unternehmen darauf möglicherweise nicht vorbereitet sind. **51 %** der Entscheider im Bereich Cybersicherheit sind der Meinung, dass derzeit **ein Mangel an Fachkräften herrscht, die ihre Anforderungen erfüllen**.



F2. Inwieweit stimmen Sie den folgenden Aussagen über Bedrohungen der Cybersicherheit in Ihrem Unternehmen zu? I Basis: 1.800

Fachkräftemangel im Bereich Cybersicherheit

Allgemein betrachtet gibt es vielerlei Gründe für den Fachkräftemangel, wobei sich keine eindeutige Ursache dafür ableiten lässt. **87 % bestätigen allerdings, dass es Probleme gibt**.



F8. Wo gibt es Ihrer Meinung im derzeitigen Talentpool Nachholbedarf, wenn es um Cybersicherheit geht? Bitte eine Antwort auswählen I Basis: 1.800

Fachkräftemangel im Bereich Cybersicherheit – nach Branche

Bei einem Blick auf die Daten aus unterschiedlichen Branchen, werden einige Unterschiede deutlich.
Aktueller Fachkräftemangel im Bereich Cybersicherheit nach Branche:

	Finanzen / Buchhaltung	Regierung / Öffentlicher Sektor	Gesundheit / Life Sciences	Medien / Unterhaltung / Reisen und Tourismus	Groß- und Einzelhandel	Technologie
Es fehlt an Erfahrung im Umgang mit großen Technologien/Unternehmen.	**18 %**	**14 %**	**18 %**	**17 %**	**12 %**	**19 %**
Es fehlt an relevanten technischen Kompetenzen.	**12 %**	**19 %**	**14 %**	**16 %**	**16 %**	**15 %**
Es fehlt ein Verständnis für die Vorgehensweise von Angreifern.	**19 %**	**18 %**	**15 %**	**13 %**	**17 %**	**15 %**
Es fehlt an Erfahrung im Umgang mit Problemen/Krisen.	**16 %**	**11 %**	**17 %**	**15 %**	**14 %**	**16 %**
Es fehlt an Erfahrung mit modernen Softwareentwicklungsmethoden.	**17 %**	**17 %**	**12 %**	**16 %**	**14 %**	**15 %**
Es fehlt an Diversität.	**5 %**	**8 %**	**8 %**	**9 %**	**9 %**	**10 %**
Es gibt keine nennenswerten Probleme mit dem derzeitigen Fachkräfteangebot im Bereich Cybersicherheit.	**14 %**	**14 %**	**16 %**	**14 %**	**19 %**	**11 %**

F8. Wo gibt es Ihrer Meinung im derzeitigen Talentpool Nachholbedarf, wenn es um Cybersicherheit geht? Bitte eine Antwort auswählen I Basis: 1.800

Wichtigste Ergebnisse

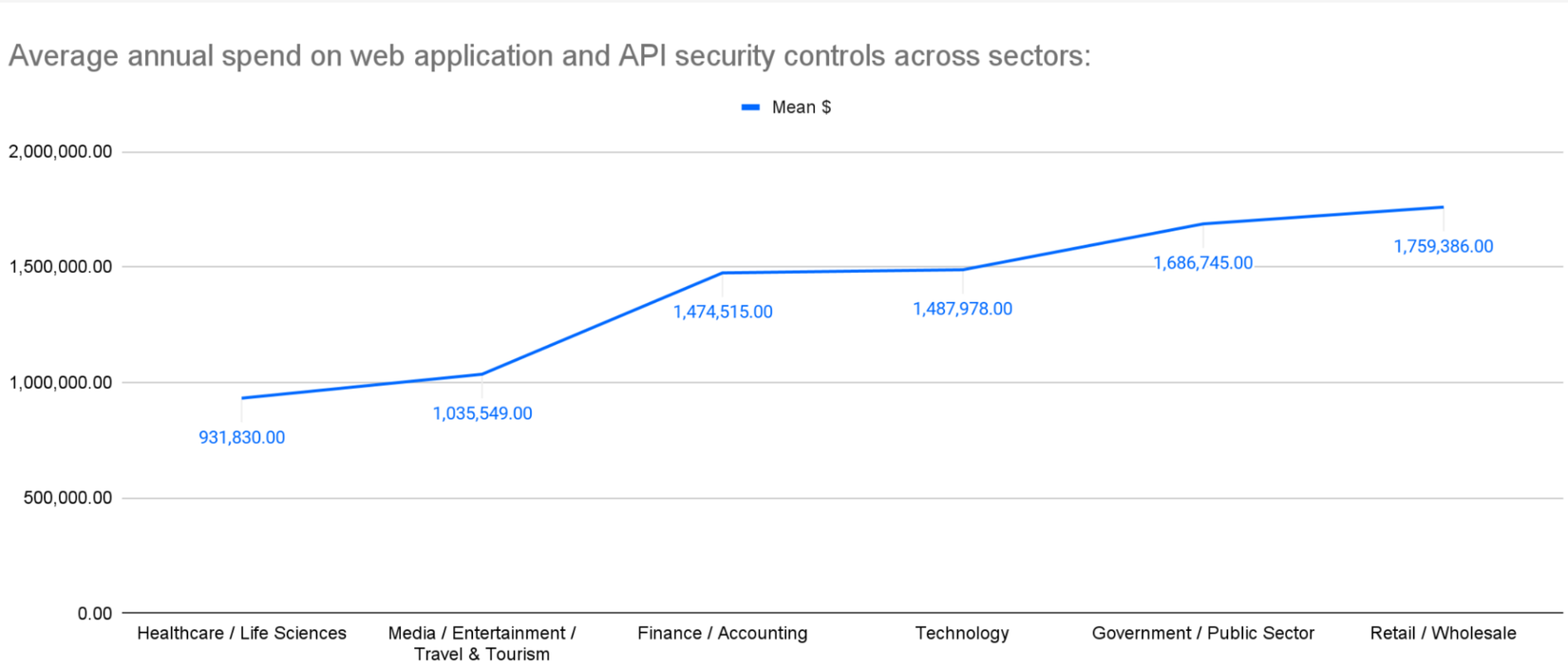
Investitionstrends im Bereich Cybersicherheit

Jährliche Ausgaben für die Sicherheit von Webanwendungen und APIs

Im Durchschnitt geben Unternehmen jährlich **1.578.475 US-Dollar** für Sicherheitskontrollen und -Tools für Webanwendungen und APIs aus. Im **Groß- und Einzelhandel** sind es sogar **1.759.386 US-Dollar**.

1.578.475 U
S-Dollar

Durchschnittlicher Betrag, der jährlich für Webanwendungs- und API-Sicherheitskontrollen/-Tools ausgegeben wird

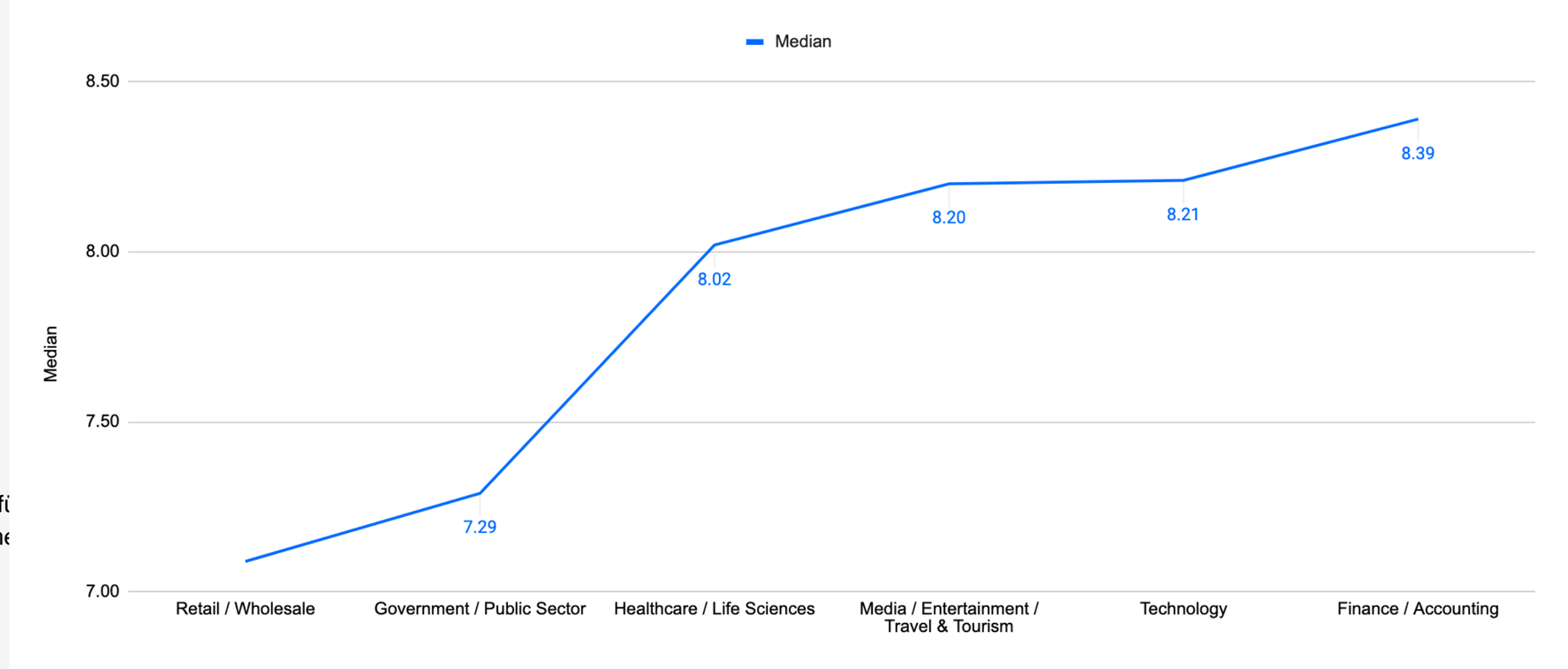


F7a. Wie hoch schätzen Sie die jährlichen Ausgaben (in US-Dollar) Ihres Unternehmens für Web-App- und API-Sicherheitsmaßnahmen und -tools? I Basis: 1.800

Anzahl der Lösungen für Netzwerk- und Anwendungssicherheit

Unternehmen verlassen sich im Durchschnitt auf **8** verschiedene Cybersicherheitslösungen.

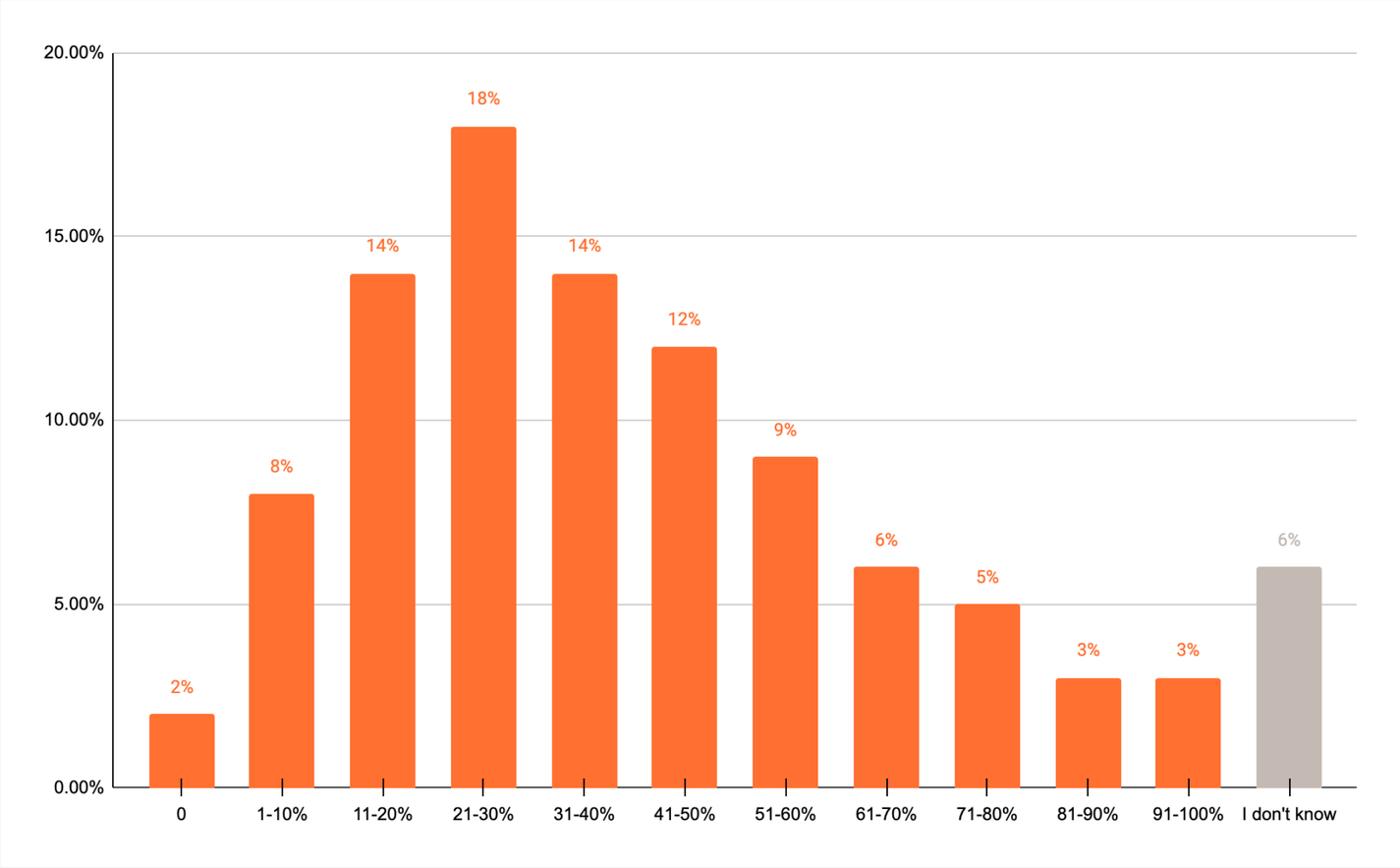
Durchschnittliche Zahl der Cybersicherheitslösungen fü
Netzwerke und Anwendungen, auf die sich Unternehme
verlassen



F7b. Auf wie viele Cybersecurity-Lösungen für die Netzwerk- und Anwendungssicherheit verlässt sich Ihr Unternehmen ungefähr? I Basis: 1.800

Überschneidungen bei den Cybersicherheitslösungen

Im Durchschnitt überschneiden sich **38 %** dieser Cybersicherheitslösungen in ihrer primären Funktion. Bei größeren Unternehmen sind es sogar 42 %.



Unternehmensgröße	Durchschnitt
250-999	37 %
1.000-4.999	36 %
5.000-24.999	38 %
>25.000	42 %

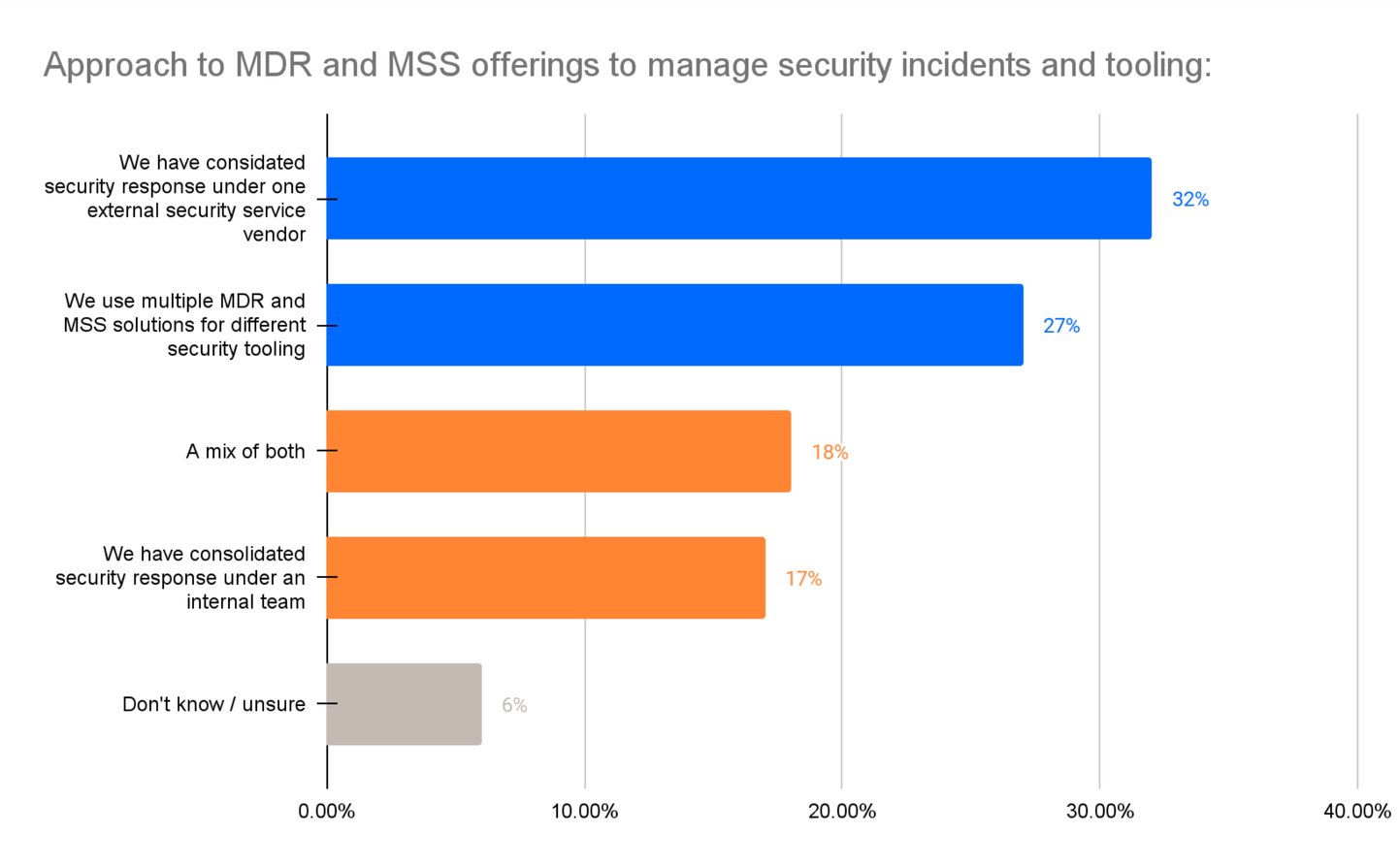
Durchschnitt: 38 %

Zunehmende Überschneidung mit der Unternehmensgröße

F7c. Wie viele dieser Lösungen überschneiden sich in etwa in ihrer primären Funktion? Bitte eine Antwort auswählen I Basis: 1.800

Herangehensweise an MDR- und MSS-Angebote zur Bewältigung von Sicherheitsvorfällen

35 % haben ihre Sicherheitsmaßnahmen bei einem externen Serviceanbieter konsolidiert, während **27 %** mehrere MDR- und MSS-Lösungen für verschiedene Sicherheitstools nutzen.



F24a. Welchen Ansatz verfolgt Ihr Unternehmen bei Managed Detection & Response (MDR)- und Managed Security Service (MSS)-Angeboten zur Verwaltung von Sicherheitsvorfällen und Sicherheitstools? Bitte eine Antwort auswählen I Basis: 1.800

Herangehensweise an MDR- und MSS-Angebote zur Bewältigung von Sicherheitsvorfällen

Häufiger zum Einsatz kommen mehrere MDR- und MSS-Lösungen anstatt einer konsolidierten Sicherheitslösung von einem einzigen Anbieter lediglich im Bereich **Finanzen / Buchhaltung**.

Sektor	Wir nutzen MDR- und MSS-Lösungen für verschiedene Sicherheitstools.	Unsere Sicherheitsmaßnahmen sind bei einem externen Anbieter von Sicherheitsservices gebündelt.
Finanzen / Buchhaltung	33 %	28 %
Regierung / Öffentlicher Sektor	15 %	29 %
Gesundheit / Life Sciences	23 %	30 %
Medien / Unterhaltung / Reisen und Tourismus	28 %	31 %
Groß- und Einzelhandel	29 %	29 %
Technologie	31 %	35 %

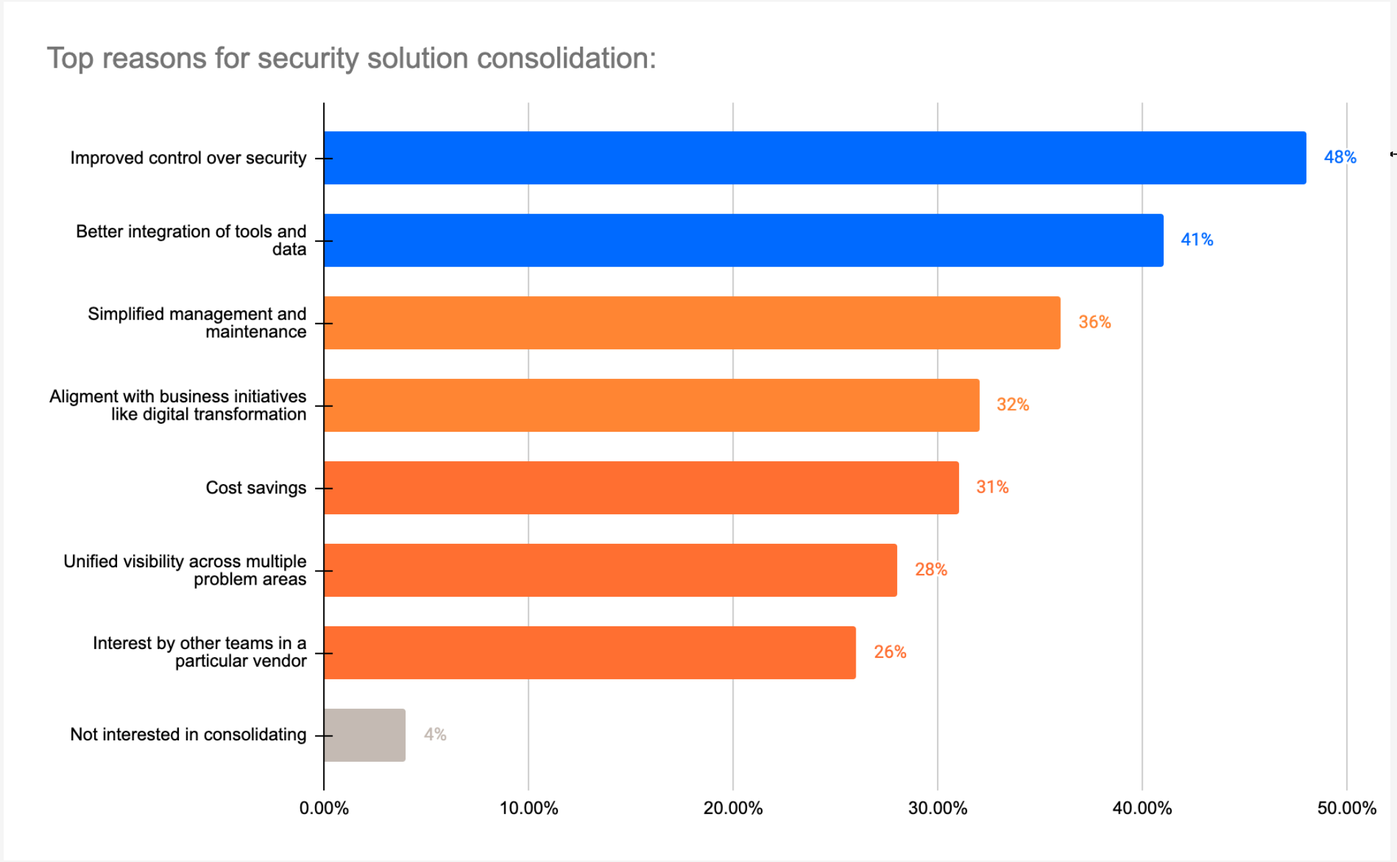
F24a. Welchen Ansatz verfolgt Ihr Unternehmen bei Managed Detection & Response (MDR)- und Managed Security Service (MSS)-Angeboten zur Verwaltung von Sicherheitsvorfällen und Sicherheitstools? Bitte eine Antwort auswählen I Basis: 1.800

Wichtigste Ergebnisse

Konsolidierung und Integration von Sicherheitslösungen

Gründe für die Konsolidierung von Sicherheitslösungen

Fast die Hälfte (48 %) führt das Interesse ihres Unternehmens an der Konsolidierung von Sicherheitslösungen auf **eine verbesserte Kontrolle über die Sicherheit** zurück, während sich weitere **41 % eine bessere Integration von Tools und Daten wünschen**.

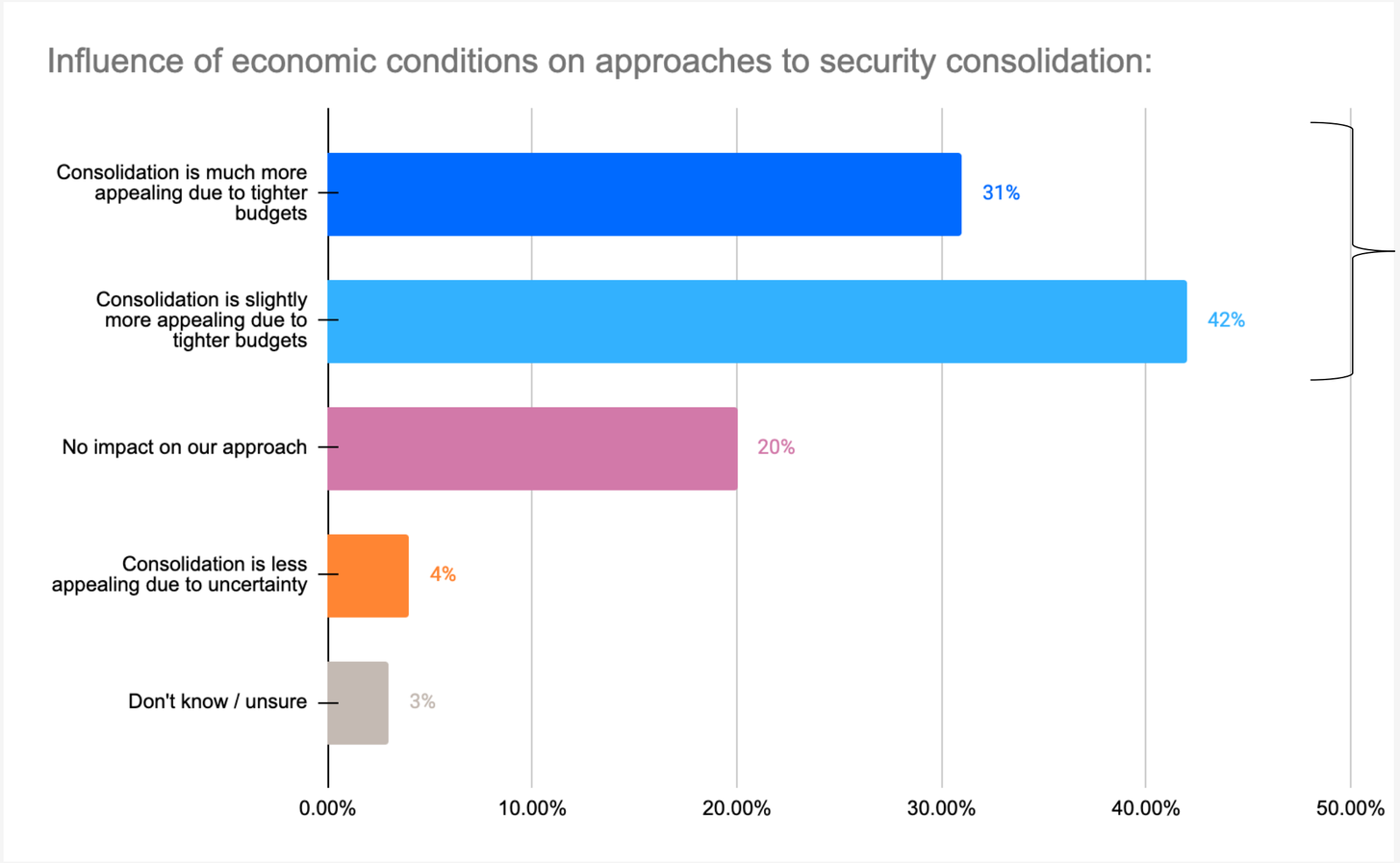


52 % in Unternehmen mit 250-999 Mitarbeitern
46 % in Unternehmen mit 1.000-4.999 Mitarbeitern

F23a. Wenn Ihr Unternehmen an einer Konsolidierung von Sicherheitslösungen interessiert ist, was sind die Hauptgründe dafür? Bitte alle zutreffenden Antworten auswählen I Basis: 1.800

Wirtschaftliche Faktoren für die Konsolidierung von Sicherheitslösungen

Fast drei Viertel (73 %) geben an, dass eine Konsolidierung von Sicherheitslösungen aufgrund immer knapperer Budgets für sie attraktiver sei.



73-prozentige Steigerung des Interesses

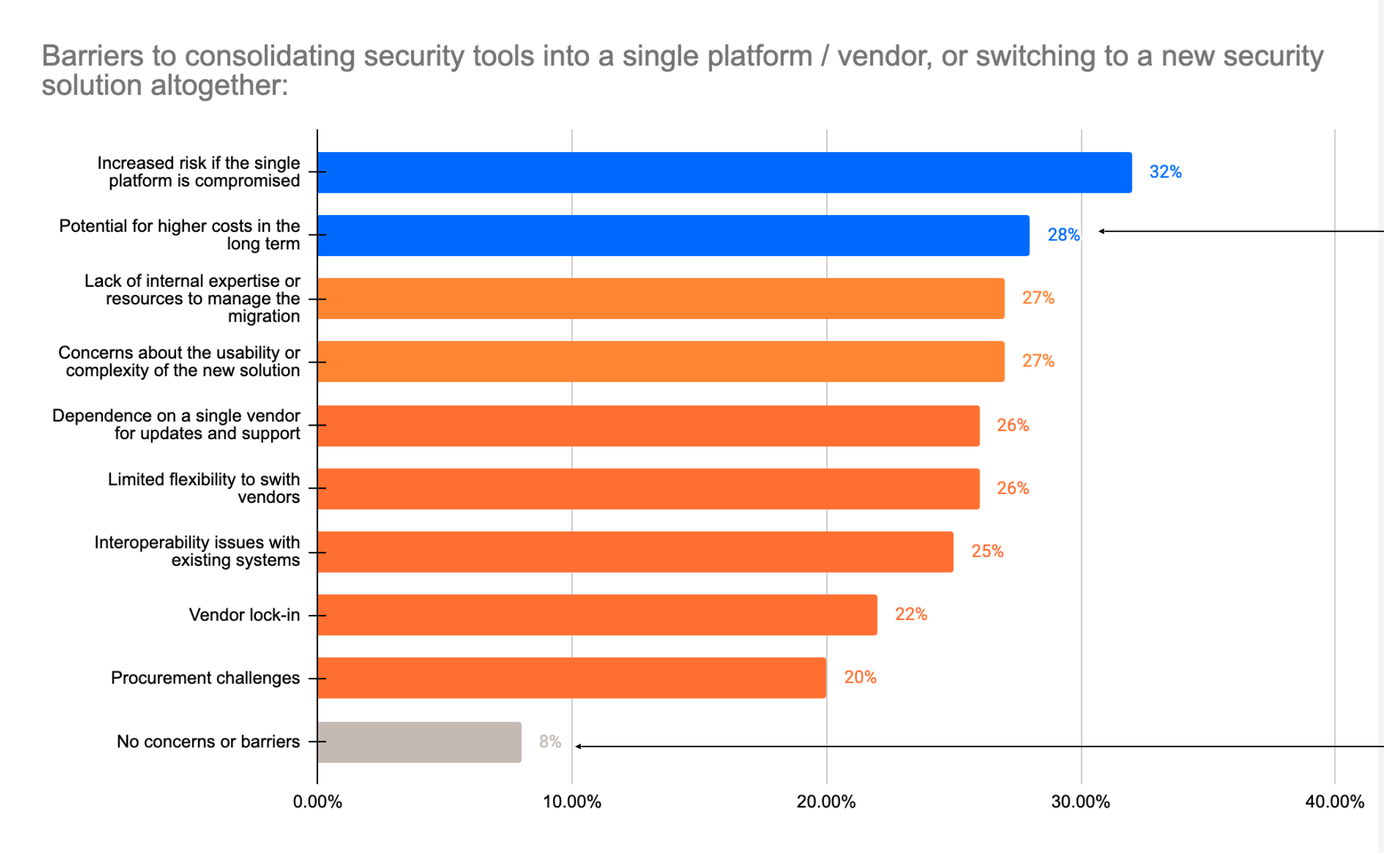
80 % Technologie

58 % Regierung / Öffentlicher Sektor

F23b. Wie hat sich die Konjunktur auf den Ansatz Ihres Unternehmens bei der Konsolidierung von Sicherheitslösungen ausgewirkt? Bitte eine Antwort auswählen I Basis: 1.726

Bedenken hinsichtlich der Konsolidierung von Sicherheitstools

Ein Drittel der Befragten (32 %) sind besorgt über das **erhöhte Risiko im Falle von Schwachstellen bei der Konsolidierung von Sicherheitstools auf einer einzigen Plattform**, dicht gefolgt von **potenziell höheren Langzeitkosten (28 %)**.



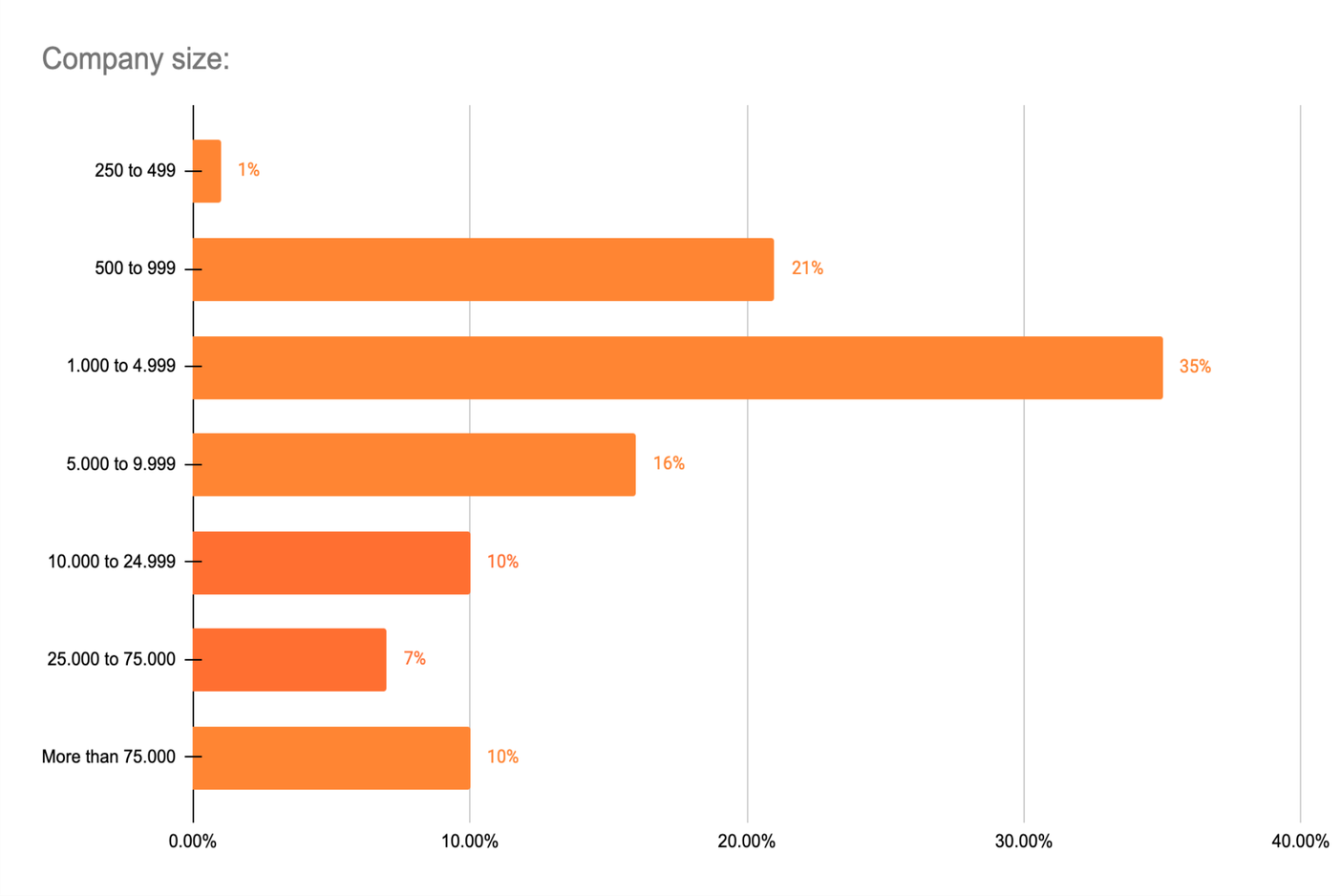
32 % in Unternehmen mit 250-999 Mitarbeitern
24 % in Unternehmen mit über 25.000 Mitarbeitern

92 % der Unternehmen haben Bedenken oder erkennen Hindernisse, wenn es um die Konsolidierung von Sicherheitstools geht.

F24b. Welche Bedenken oder Hindernisse gibt es bei der Konsolidierung Ihrer Sicherheitstools auf einer einzigen Plattform/bei einem einzigen Anbieter oder beim Wechsel zu einer neuen Sicherheitslösung? Bitte alle zutreffenden Antworten auswählen I Basis: 1.800

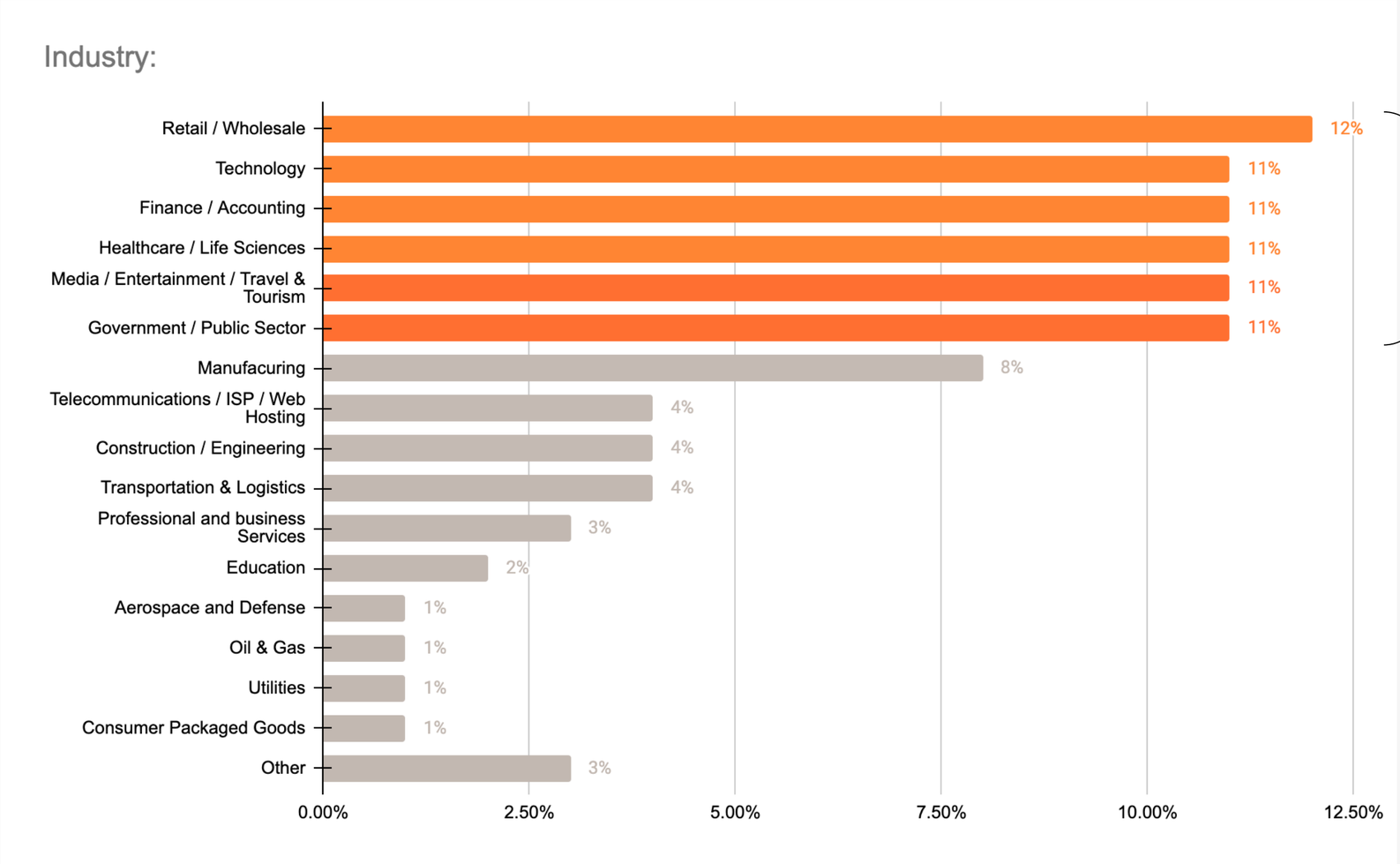
Demografische Daten

Unternehmensgröße



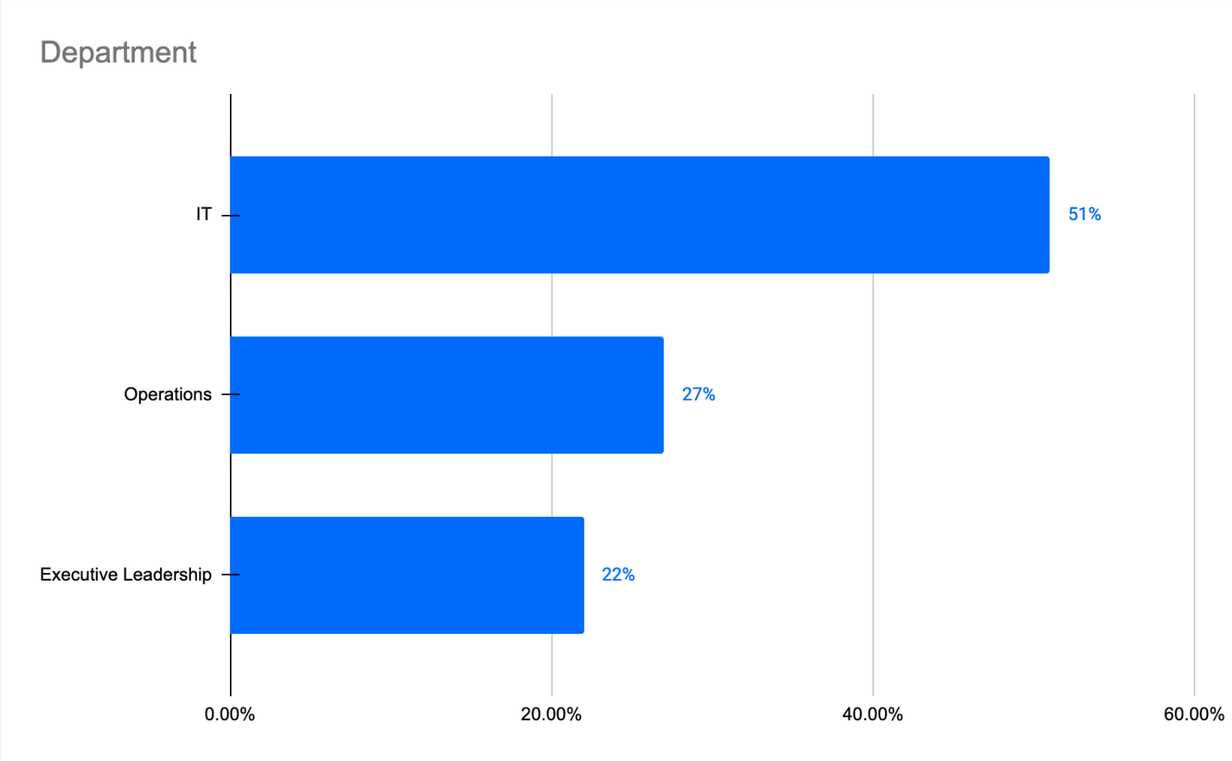
S2. Wie viele Mitarbeiter sind in Ihrem Unternehmen beschäftigt? Bitte 1 Antwort auswählen

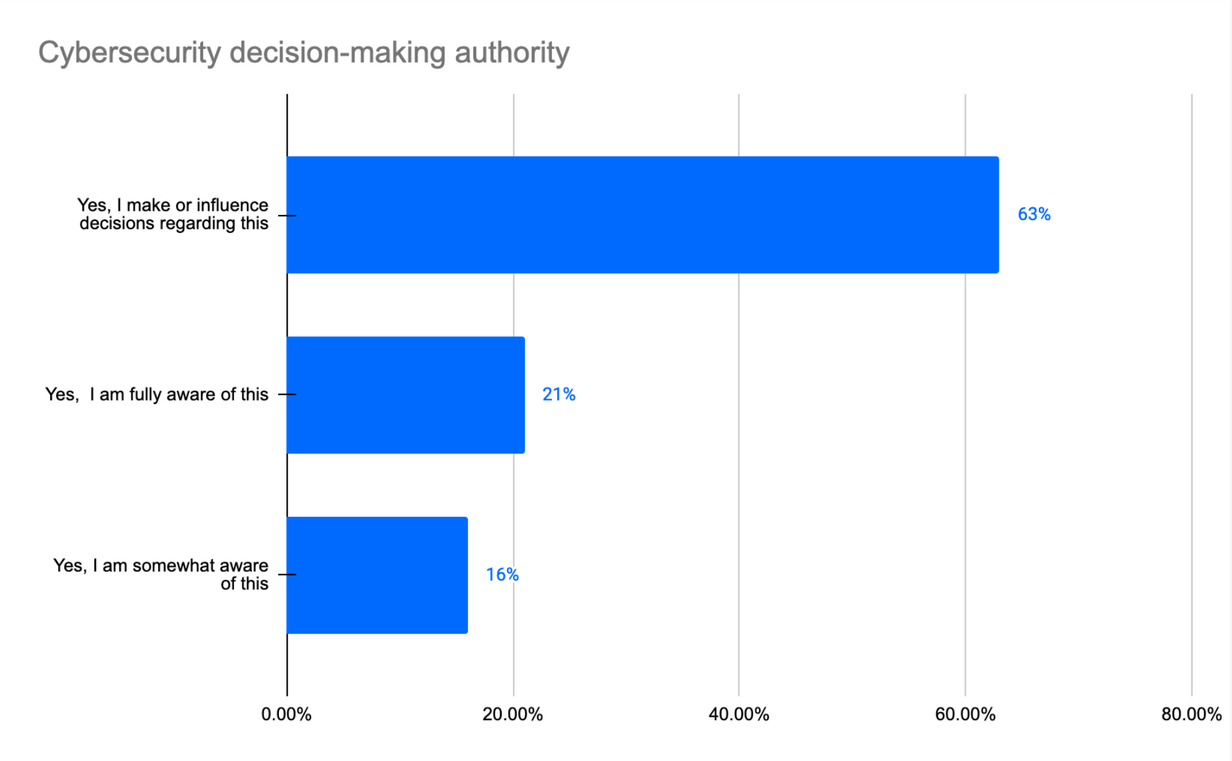
Branche



S3. Welche der folgenden Antworten beschreibt die Branche, in der Ihr Unternehmen tätig ist, am besten? Bitte eine Antwort auswählen I Basis: 1.800

Abteilung und Befugnisse





S4. Welche der folgenden Antworten beschreibt am besten die Abteilung, in der Sie tätig sind? Bitte 1 Antwort auswählen
S5. Wissen Sie im Rahmen Ihrer derzeitigen Aufgaben über Entscheidungen zum Thema Cybersicherheit in Ihrem Unternehmen Bescheid oder treffen oder beeinflussen Sie solche Entscheidungen? Bitte eine Antwort auswählen | Basis: 1.800

Vielen Dank!