Weltweite Studie zum Thema Security 2024

Ergebnisse DACH

November 2024

Durchführung der Studie:
SAPIO Research

Übersicht und Methodik

Die Umfrage wurde unter **200 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 in der DACH-Region** 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 ±6,9 % um den wahren Wert.

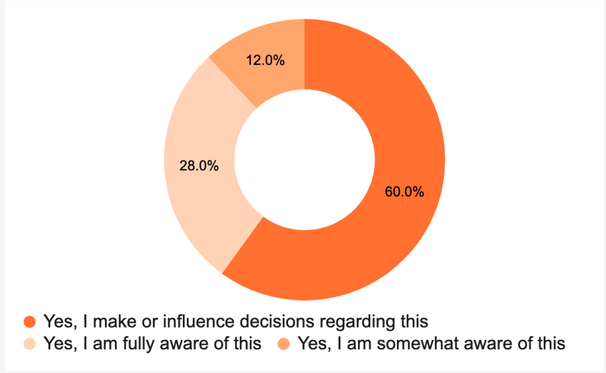
Die Befragungen wurden von Sapio Research im September 2024 per Onlineumfrage mittels E-Mail-Einladung durchgeführt.

Die demografischen Daten der Cybersicherheitsentscheider im Überblick

Führungsgrad

Abteilung	% der Befragten
IT	49 %
Operations	29 %
Obere Führungsriege	23 %

Entscheidungskompete



Führungsgrad

Anz. Beschäftigte	% der Befragten
250-999	21 %
1.000-4.999	35 %
5.000-24.999	26 %
25.000+	17 %

Primärer Wirtschaftszweig

1. Finanzen / Buchhaltung – 18 %
2. Medien / Unterhaltung / Reisen und Tourismus – 16 %
3. Groß- und Einzelhandel – 15 %
4. Gesundheit / Life Sciences – 14 %
5. Fertigung – 7 %
6. Telekommunikation / ISP / Webhosting – 7 %

Wohnsitzland

Fazit

Wichtige Statistiken

Für die Erholung von Sicherheitsvorfällen werden von Unternehmen **6,47 Monate** veranschlagt.

Im vergangenen Jahr waren Unternehmen im Durchschnitt von **41** Sicherheitsvorfällen betroffen. Hauptursachen waren **externe Angreifer** (36 %) und **Fehlkonfigurationen** (29 %).

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

Unternehmen gehen davon aus, dass **Social-Engineering-Angriffe** (38 %) und ein **Mangel an relevanten technischen Kompetenzen** (31 %) in den nächsten 12 Monaten die größten Bedrohungen für ihre Cybersicherheit darstellen werden.

Umsatzeinbußen gehörten zu den Hauptfolgen von Sicherheitsvorfällen **(22 %)**, wobei der durchschnittliche Verlust **3,3 %** betrug.

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

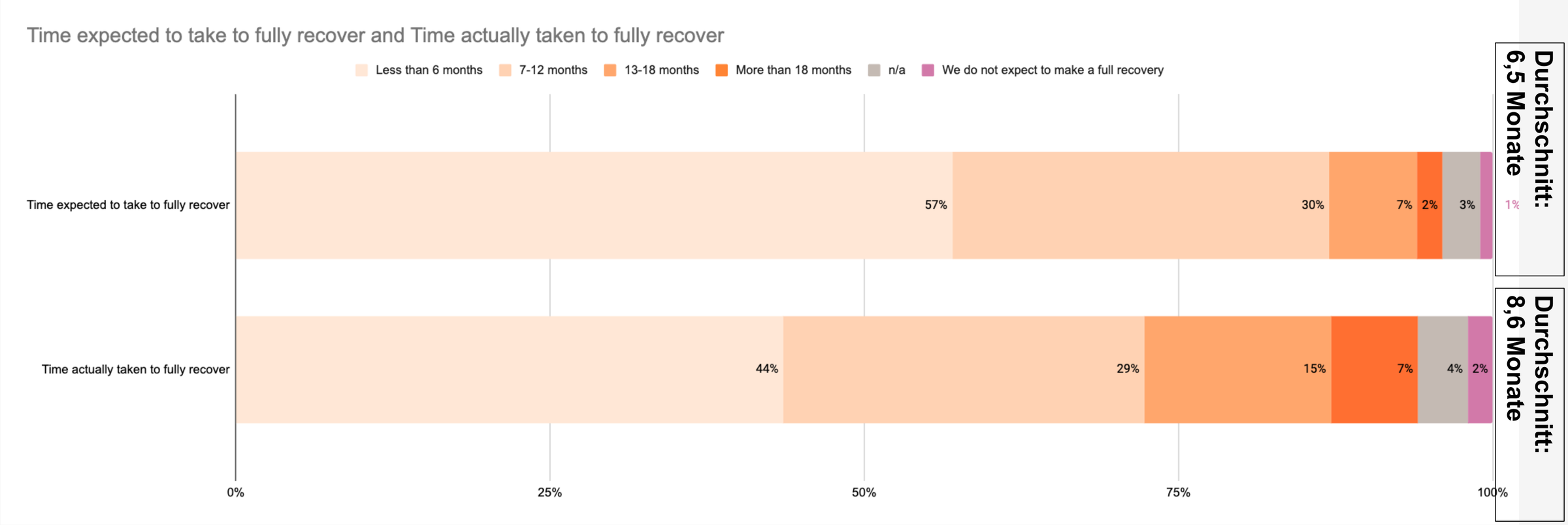
Wichtigste Ergebnisse

Wichtigste Ergebnisse

Reaktions- und Wiederherstellungszeit bei Sicherheitsvorfällen

Erwartete vs. tatsächliche Wiederherstellungszeit nach einem Sicherheitsvorfall

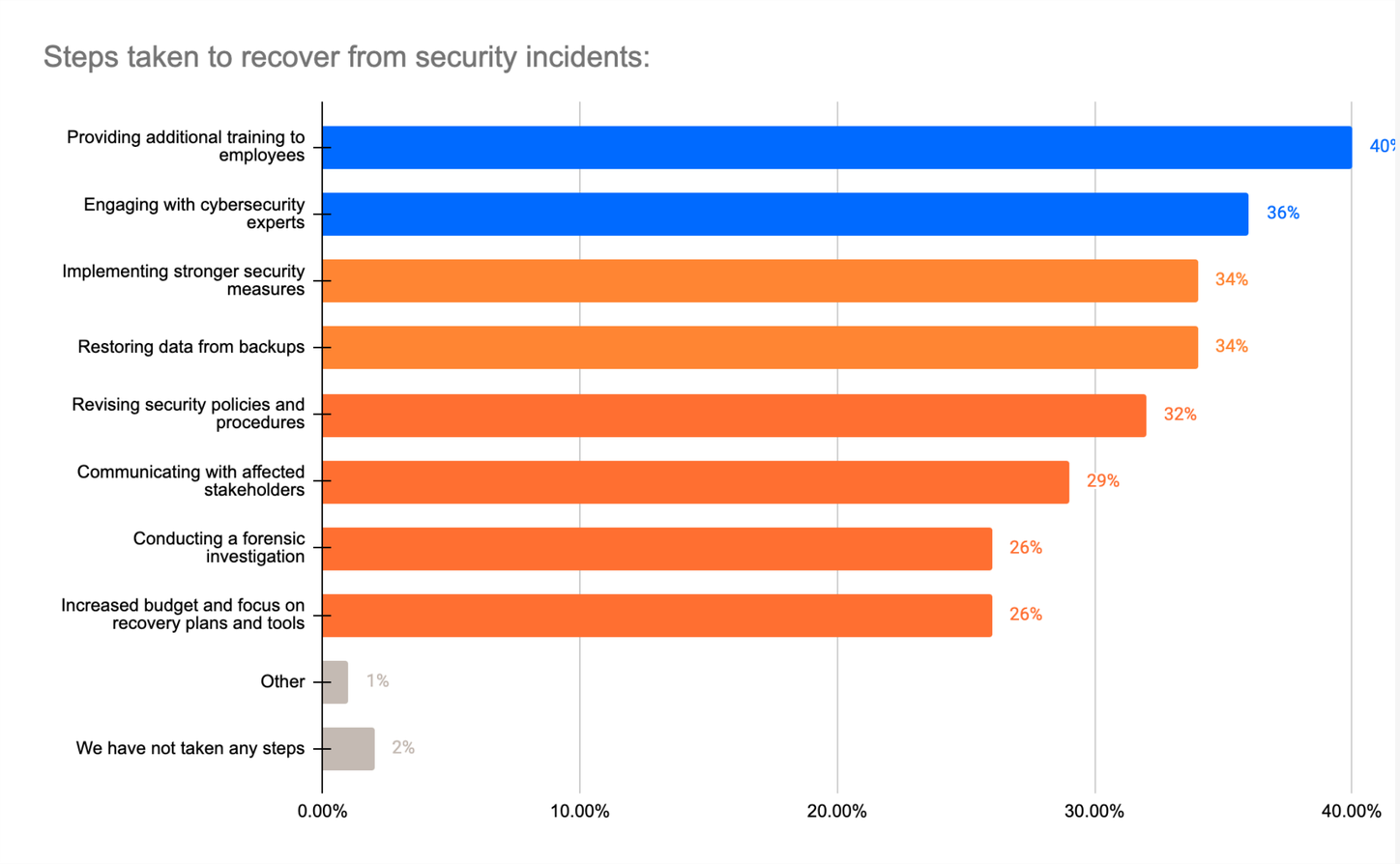
Die durchschnittliche Zeit, die Unternehmen benötigen, um sich von einem Sicherheitsvorfall zu erholen, beträgt 8,6 Monate – 2,1 Monate länger als im Durchschnitt von Unternehmen erwartet.



F17e. Wie lange hat es gedauert, bis Sie sich von diesen Auswirkungen vollständig erholt hatten, oder wie lange wird es voraussichtlich dauern? I Basis: 183
* Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Schritte zur Erholung von Sicherheitsvorfällen

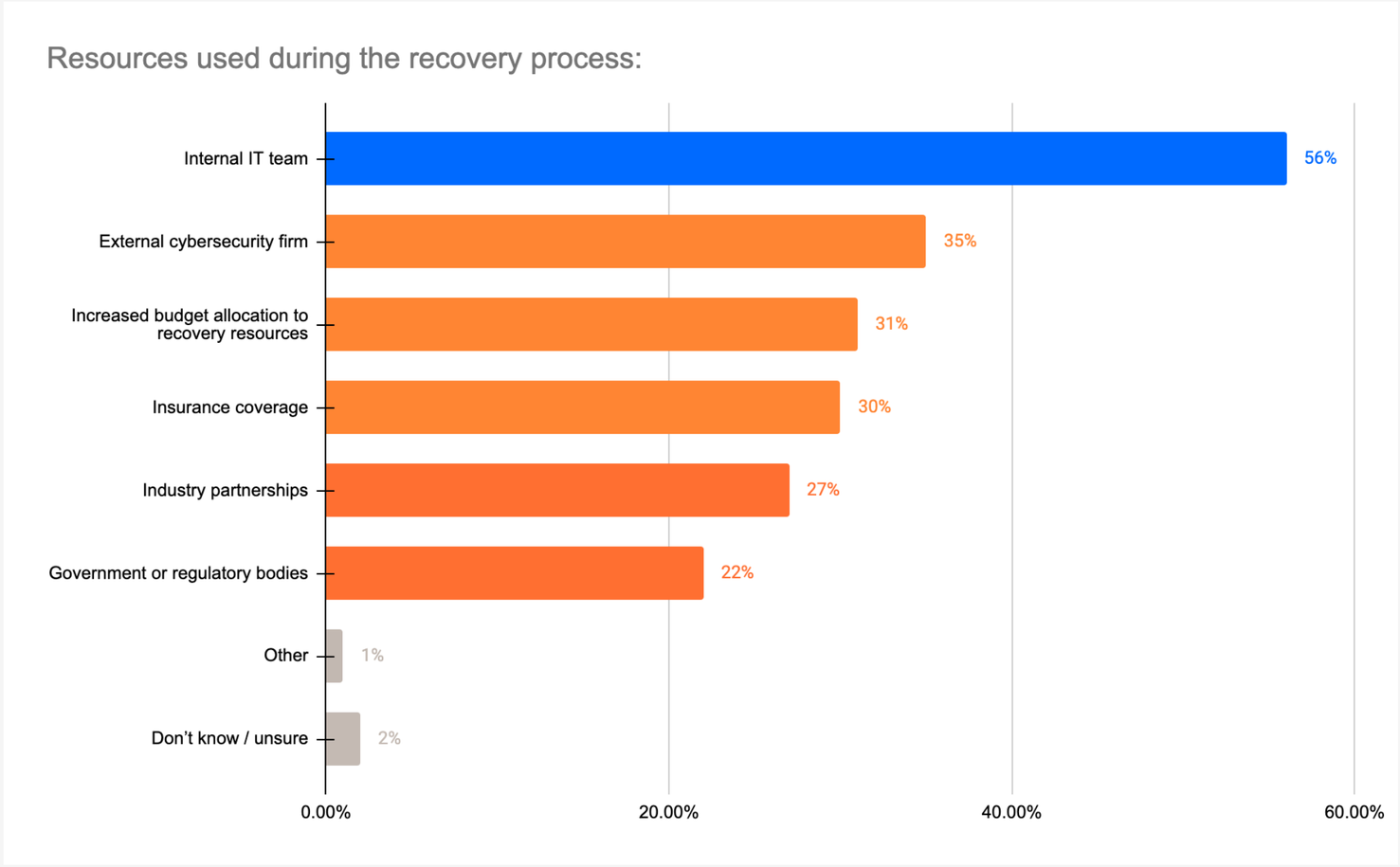
Die häufigsten Maßnahmen, die Unternehmen zur Erholung von Sicherheitsvorfällen ergreifen, sind zusätzliche Mitarbeiterschulungen (40 %) und die Zusammenarbeit mit Cybersicherheitsexperten (36 %).



F18. Welche Schritte hat Ihr Unternehmen unternommen, um sich von dem Sicherheitsvorfall zu erholen? Bitte alle zutreffenden Antworten auswählen I Basis: 183 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Für die Erholung von Sicherheitsvorfällen aufgewendete Ressourcen

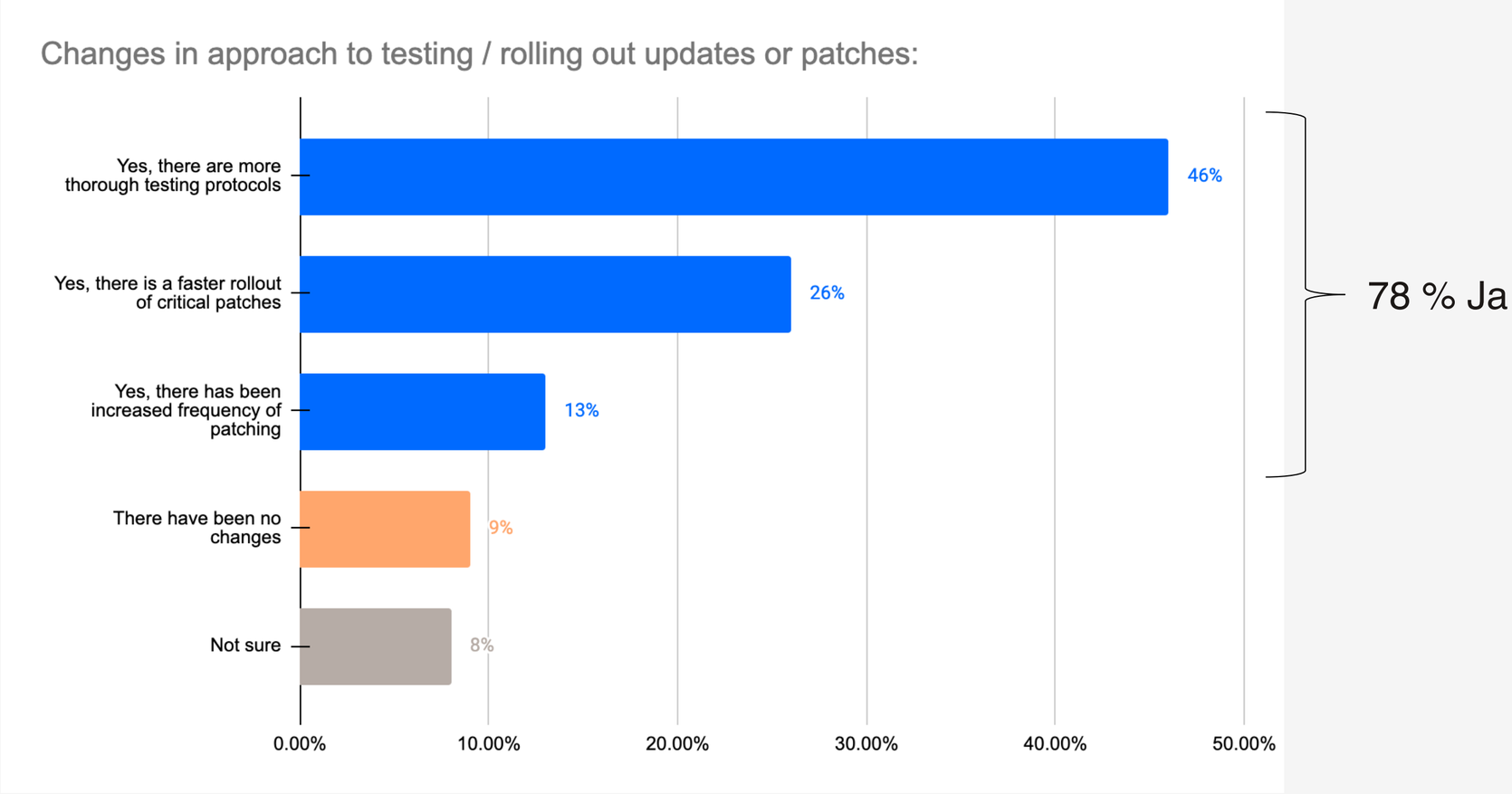
Die meisten Unternehmen setzen ihr internes IT-Team (56 %) bei der Erholung von Sicherheitsvorfällen ein.



F19. Welche Ressourcen hat Ihr Unternehmen bei der Erholung von Sicherheitsvorfällen genutzt? Bitte alle zutreffenden Antworten auswählen I Basis: 180 (Es wurden nur diejenigen Unternehmen befragt, die bereits Schritte zur Erholung von Sicherheitsvorfällen ergriffen hatten.)

Änderungen in der Vorgehensweise bei Updates und Patch-Tests

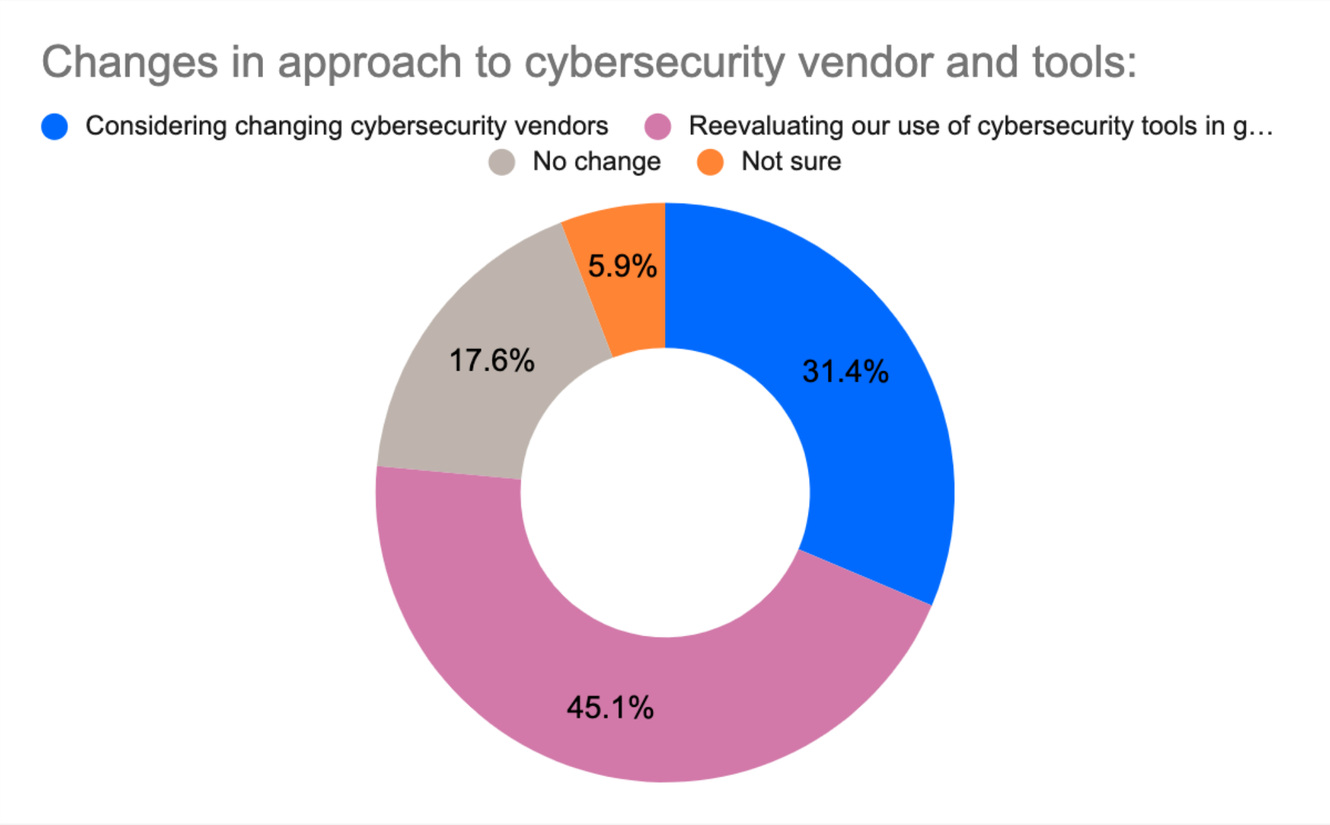
84 % der Befragten geben an, dass die jüngsten Probleme mit der Zuverlässigkeit ihr Unternehmen dazu veranlasst haben, ihre Vorgehensweise beim Testen oder der Einführung von Updates oder Patches zu ändern.



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: 200

Umgang mit Cybersicherheitsanbietern und -Tools

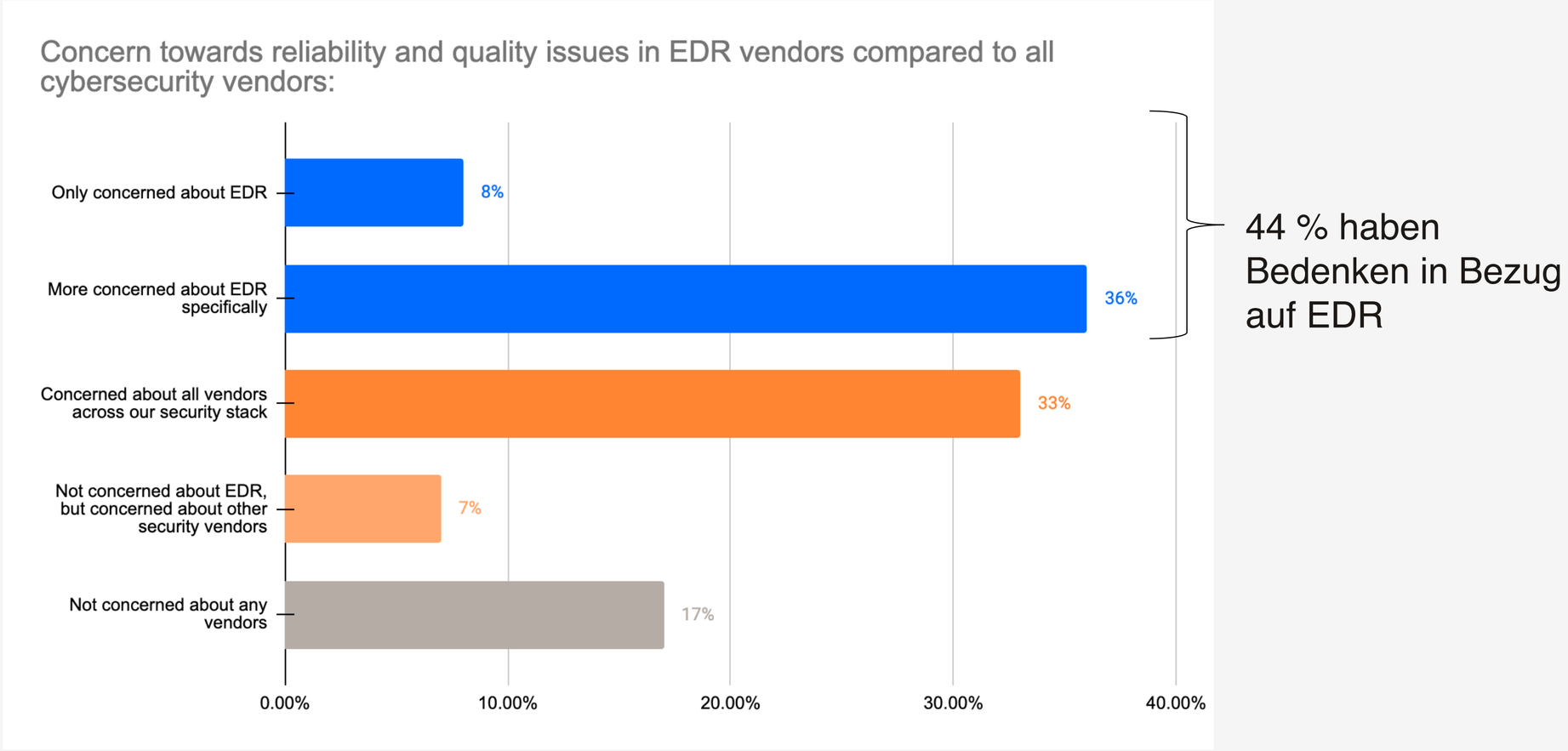
46 % überdenken nach dem jüngsten Crowdstrike Ausfall die Nutzung von Cybersicherheitstools im Allgemeinen, und weitere 32 % erwägen einen Anbieterwechsel.



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: 200

Bedenken hinsichtlich der Zuverlässigkeit von EDR-Anbietern

83 % sind besorgt über die Zuverlässigkeit und Qualität ihrer Anbieter, wobei manche Befragten Bedenken in Bezug auf alle Anbieter in ihrem Sicherheitsstack haben (33 %) und manche nur in Bezug auf EDR-Anbieter (44 %).



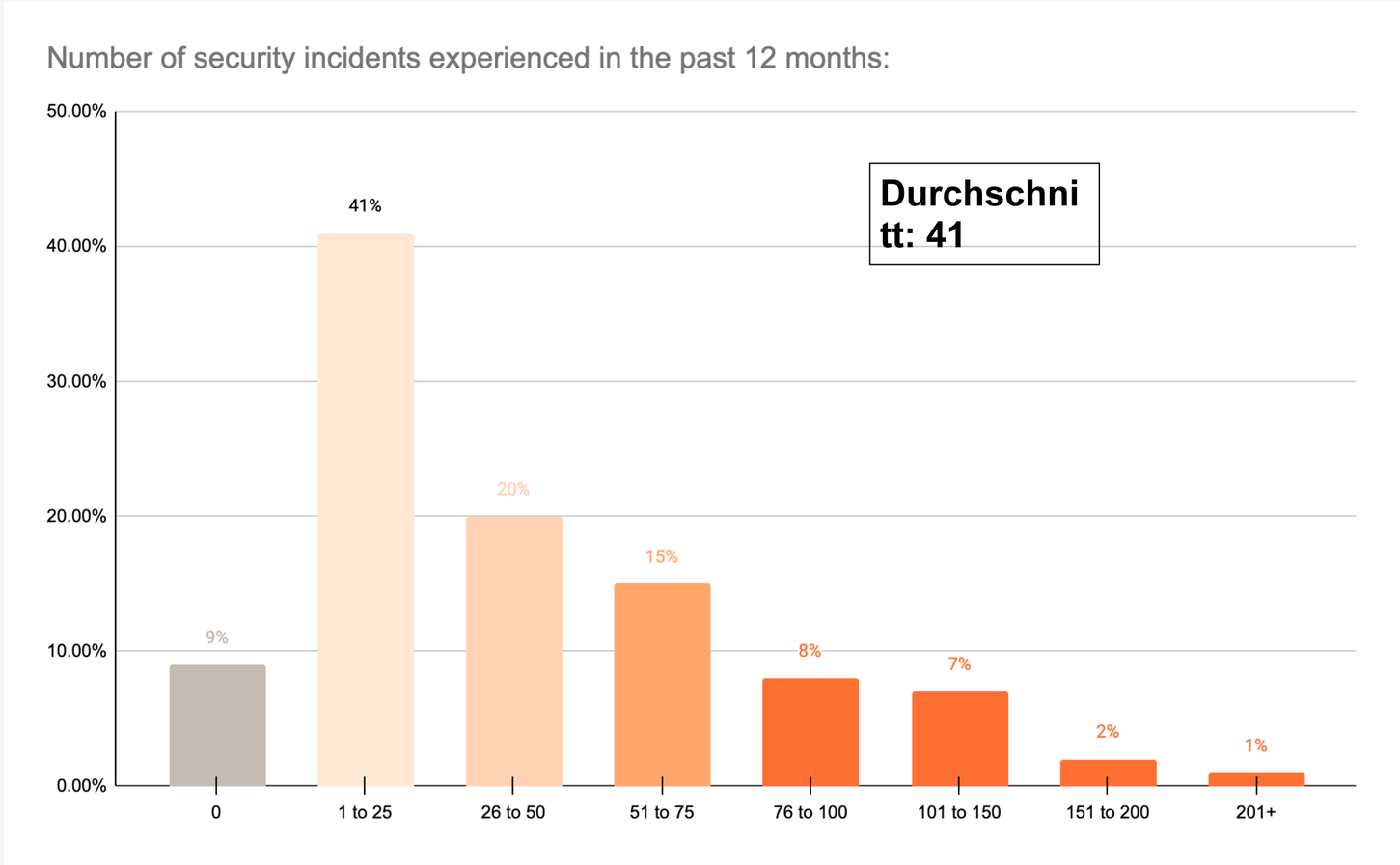
F22a. Inwiefern sind Sie angesichts des Crowdstrike Ausfalls besorgt über die Zuverlässigkeit und Softwarequalität von EDR-Anbietern im Vergleich zu anderen Anbietern von Cybersicherheitsprodukten? Bitte eine Antwort auswählen I Basis: 200

Wichtigste Ergebnisse

Die Bedrohungslage

Anzahl der Sicherheitsvorfälle im vergangenen Jahr

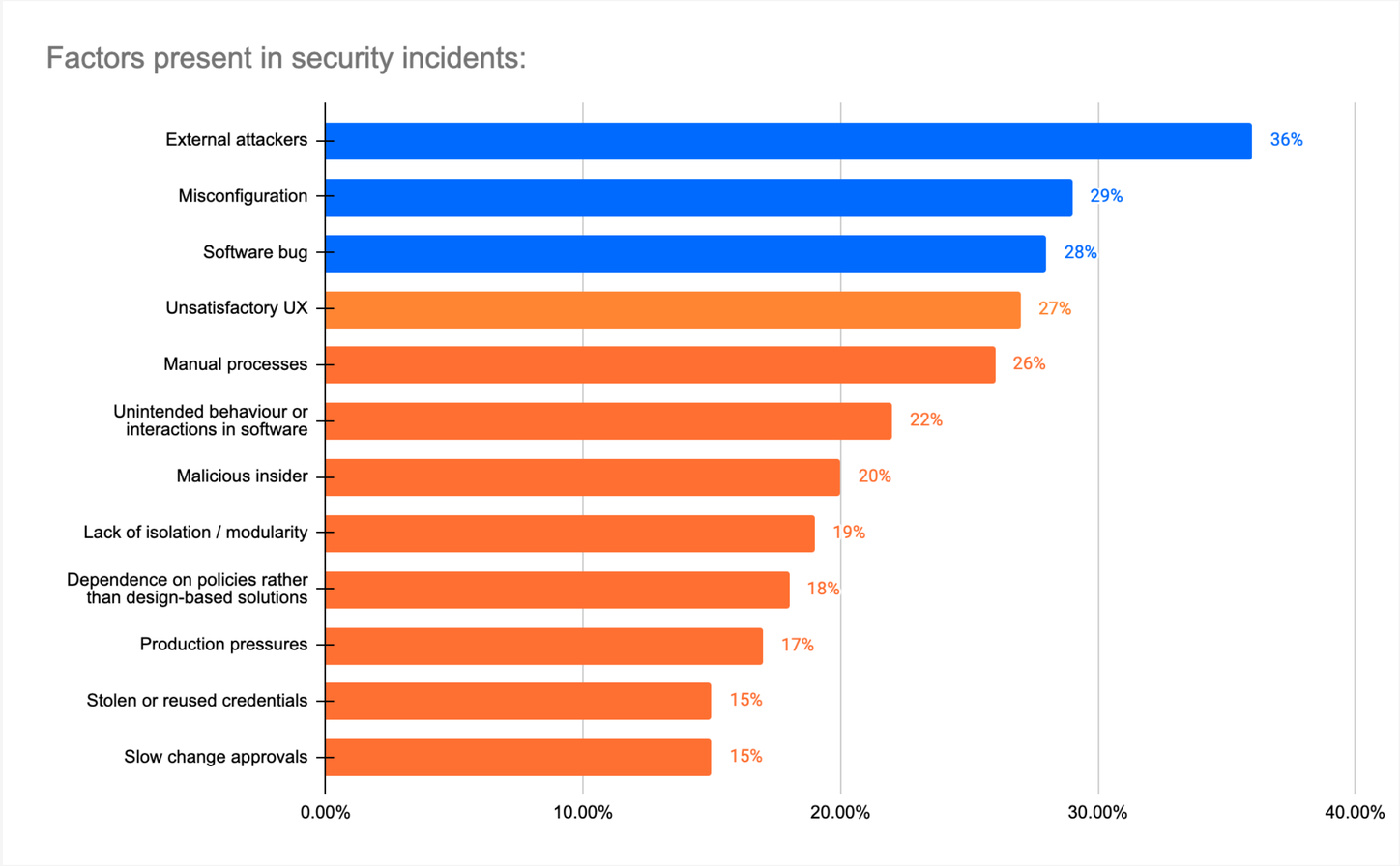
Im Durchschnitt waren Unternehmen in den letzten 12 Monaten von 41 Sicherheitsvorfälle betroffen.



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: 200

Faktoren, die bei Sicherheitsvorfällen eine Rolle spielen

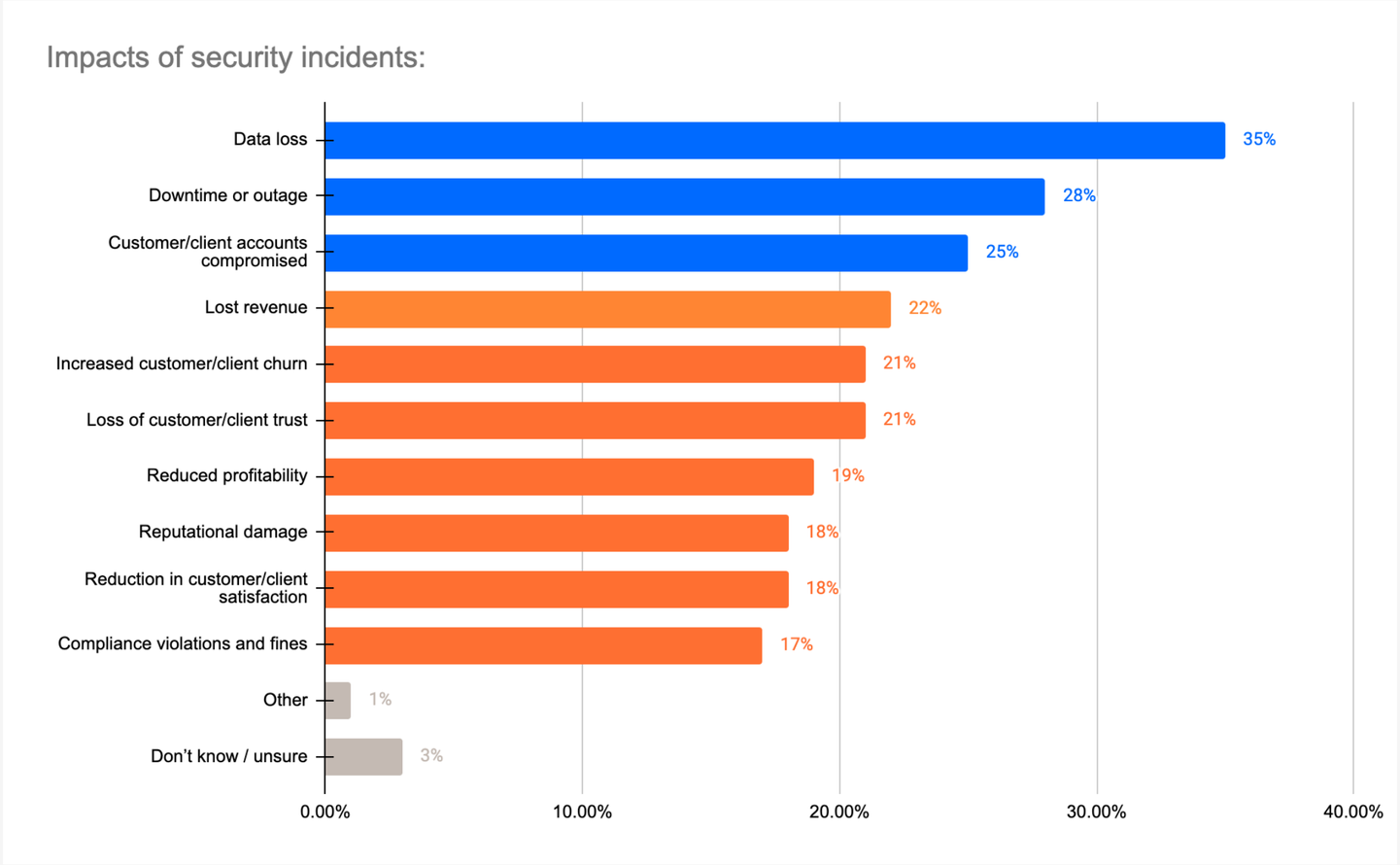
Zu den wichtigsten Faktoren, die bei Sicherheitsvorfällen eine Rolle spielen, gehören externe Angreifer (36 %), Fehlkonfigurationen (29 %) und Softwarefehler (28 %).



F16. Welche der folgenden Faktoren spielten bei dem Sicherheitsvorfall eine Rolle? Bitte alle zutreffenden Antworten auswählen I Basis: 183 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Hauptfolgen von Sicherheitsvorfällen

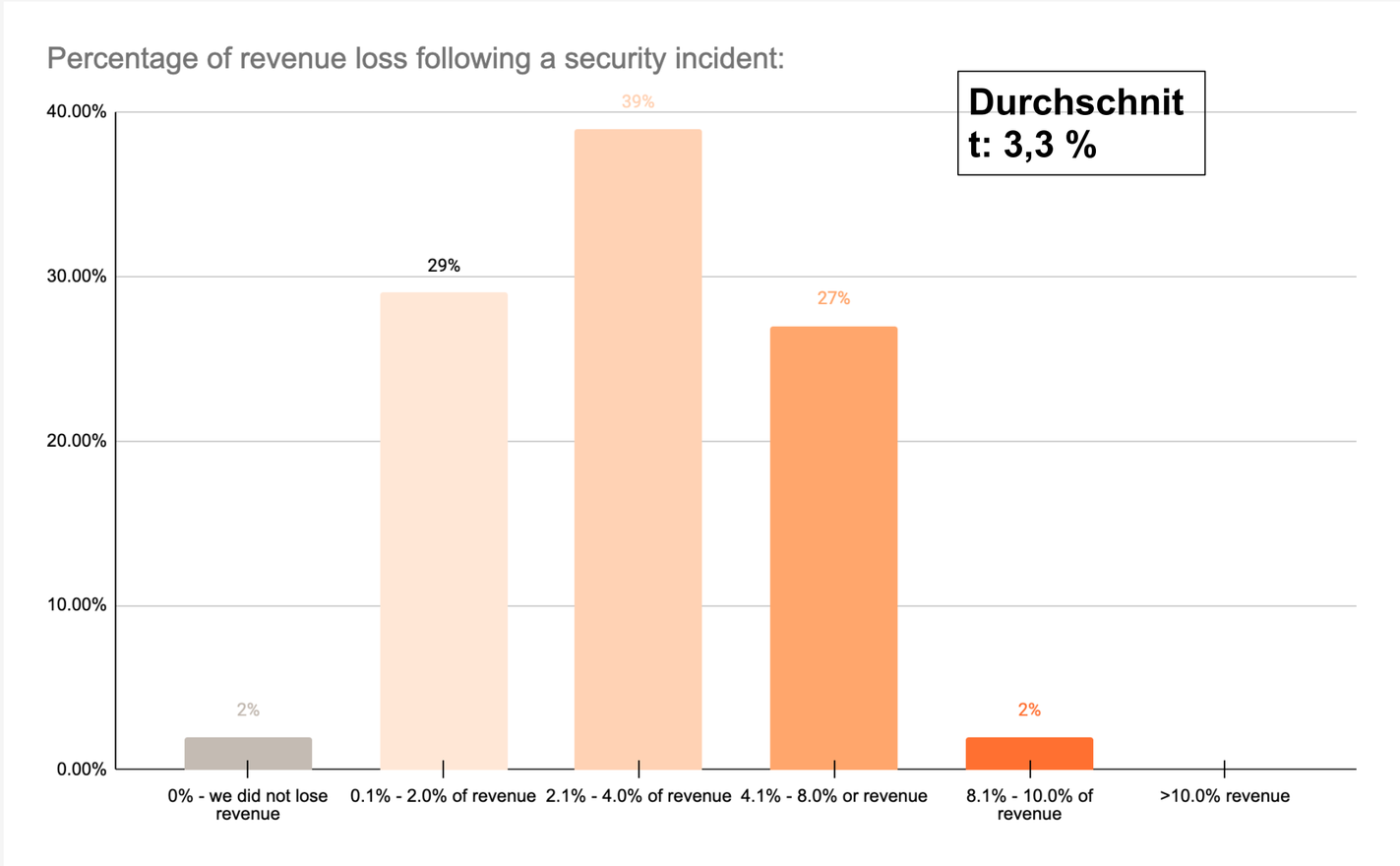
Zu den Hauptfolgen von Sicherheitsvorfällen gehören Datenverluste (35 %), Ausfallzeiten (28 %) und die Gefährdung von Kundenkonten (25 %).



F17a. Was waren die Hauptfolgen des Sicherheitsvorfalls? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 183 * Es wurden nur diejenigen Studienteilnehmer befragt, die in den letzten 12 Monaten von einem Sicherheitsvorfall betroffen waren.

Umsatzeinbußen aufgrund von Sicherheitsvorfällen

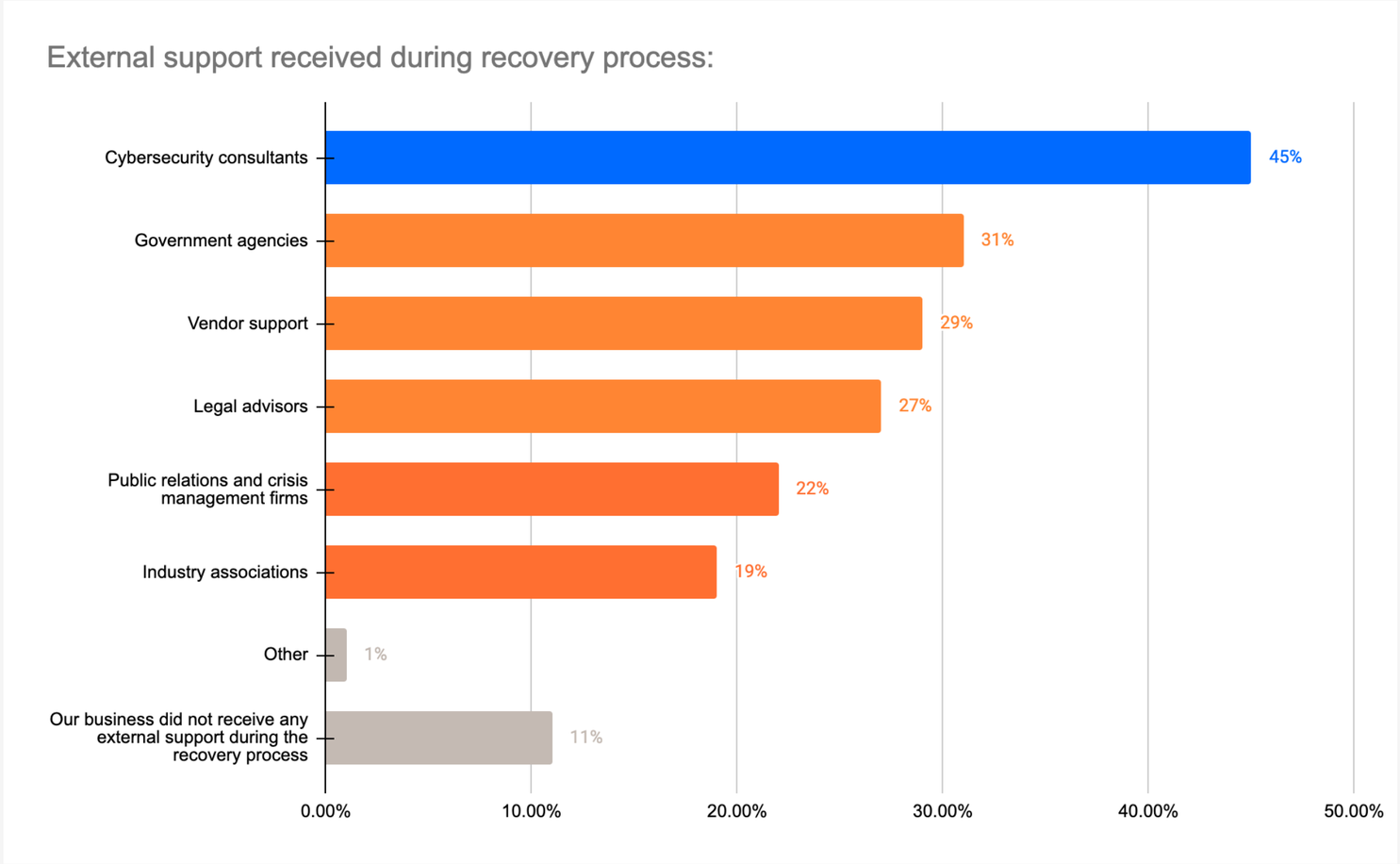
Diejenigen Befragten, die Umsatzeinbußen als Hauptfolge von Sicherheitsvorfällen angeben, berichten von einem durchschnittlichen Umsatzverlust von 3,3 %.



F17b. Wie viel Prozent Ihres Umsatzes mussten Sie aufgrund eines Sicherheitsvorfalls ungefähr einbüßen? Bitte eine Antwort auswählen I Basis: 41 * Es wurden nur diejenigen Unternehmen befragt, die in Folge eines Sicherheitsvorfalls Umsätze einbüßen mussten.

Externe Unterstützung bei der Erholung von Sicherheitsvorfällen

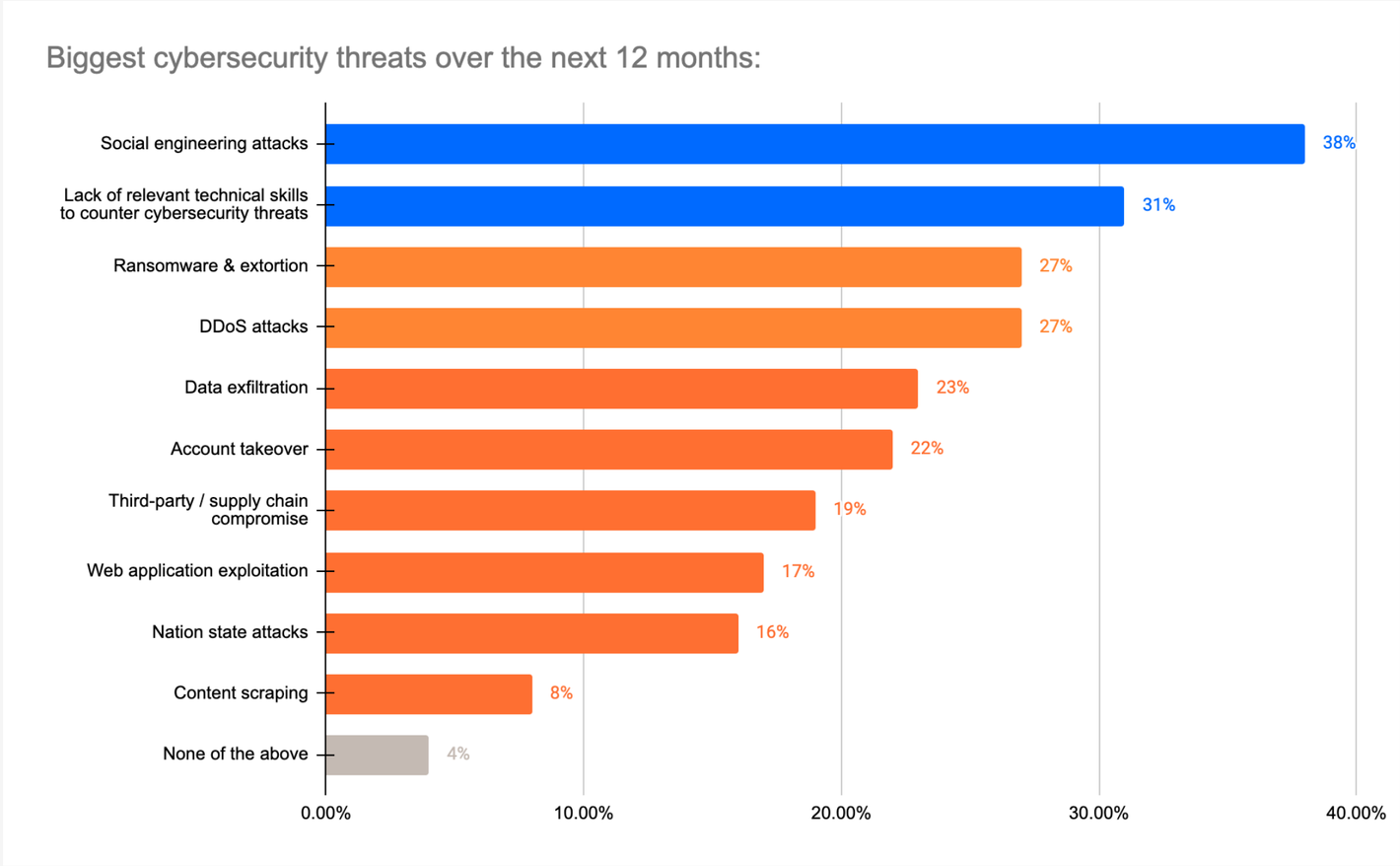
45 % geben an, dass ihr Unternehmen bei der Erholung von Sicherheitsvorfällen externe Hilfe in Anspruch genommen hat.



F22b. Welche externe Unterstützung oder Hilfe hat Ihr Unternehmen bei der Erholung von Sicherheitsvorfällen erhalten (falls zutreffend)? Bitte alle zutreffenden Antworten auswählen I Basis: 200

Größte prognostizierte Bedrohungen für die Cybersicherheit

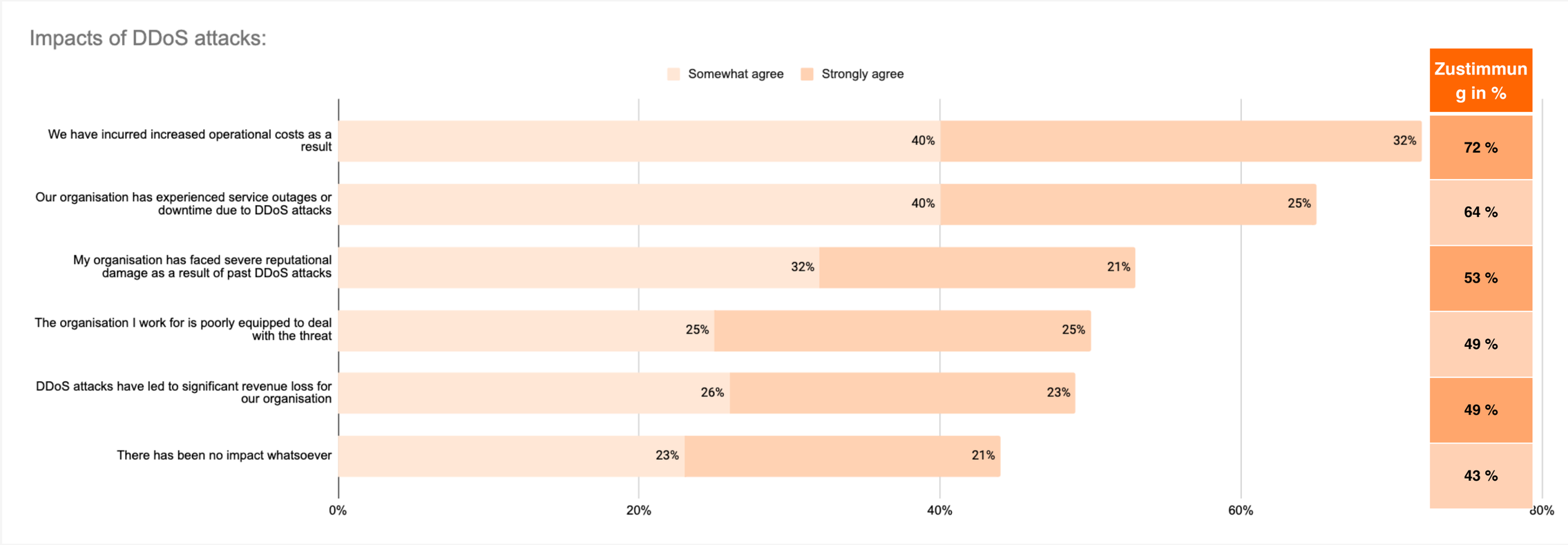
Unternehmen gehen davon aus, dass Social-Engineering-Angriffe (38 %) und ein Mangel an relevanten technischen Kompetenzen (31 %) in den nächsten 12 Monaten die größten Bedrohungen für ihre Cybersicherheit darstellen werden.



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: 200

Auswirkungen von DDoS-Angriffen

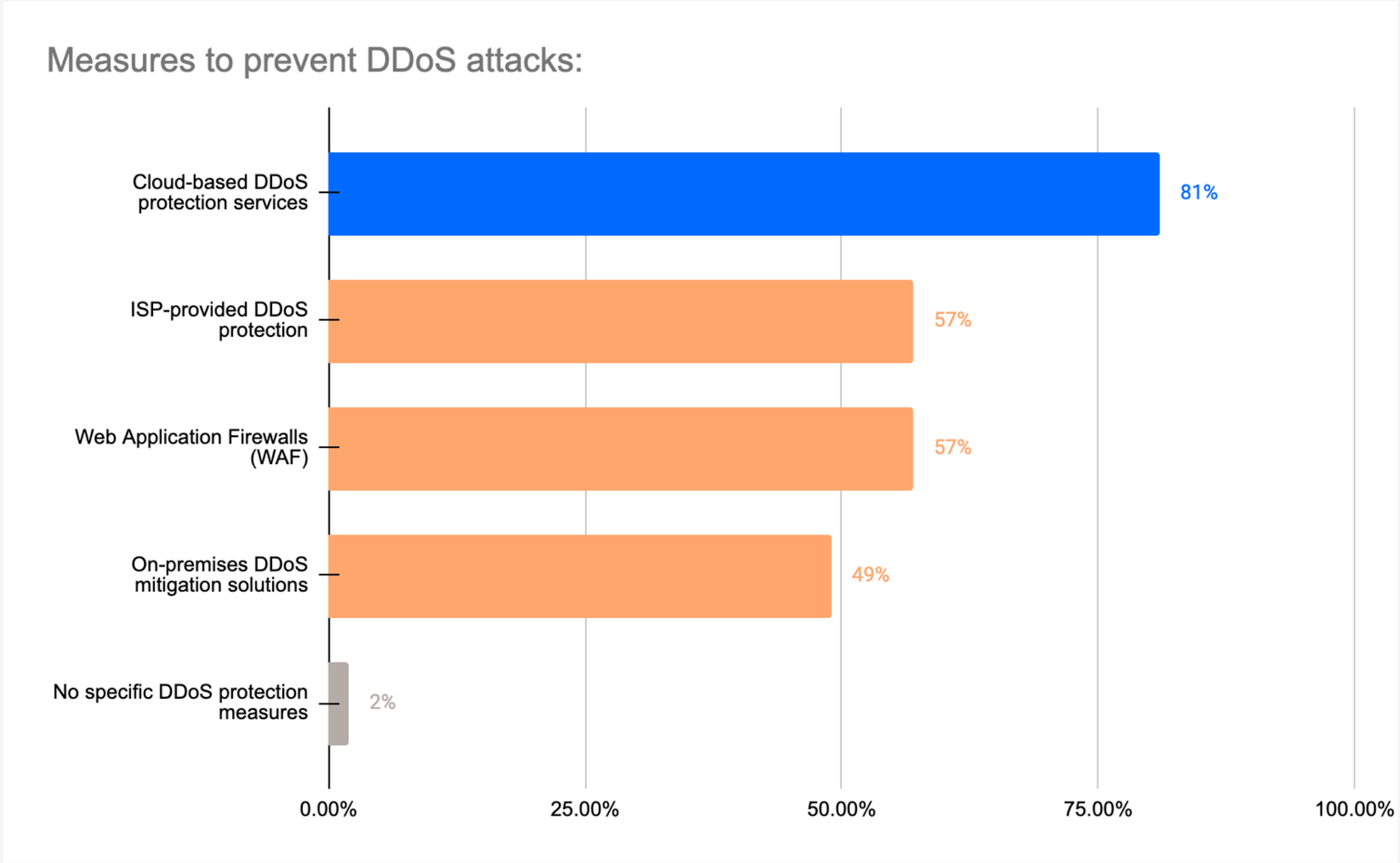
Entscheider, die glauben, dass DDoS-Angriffe in den nächsten 12 Monaten zu den größten Bedrohungen gehören werden, lassen sich voraussichtlich von den erheblichen negativen Auswirkungen von DDoS-Angriffen leiten: 72 % sagen, dass diese zu erhöhten Betriebskosten führen.



F1b. Inwiefern stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 53 * Es wurden nur diejenigen befragt, die glauben, dass DDoS-Angriffe eine Bedrohung darstellen.

DDoS-Schutzmaßnahmen

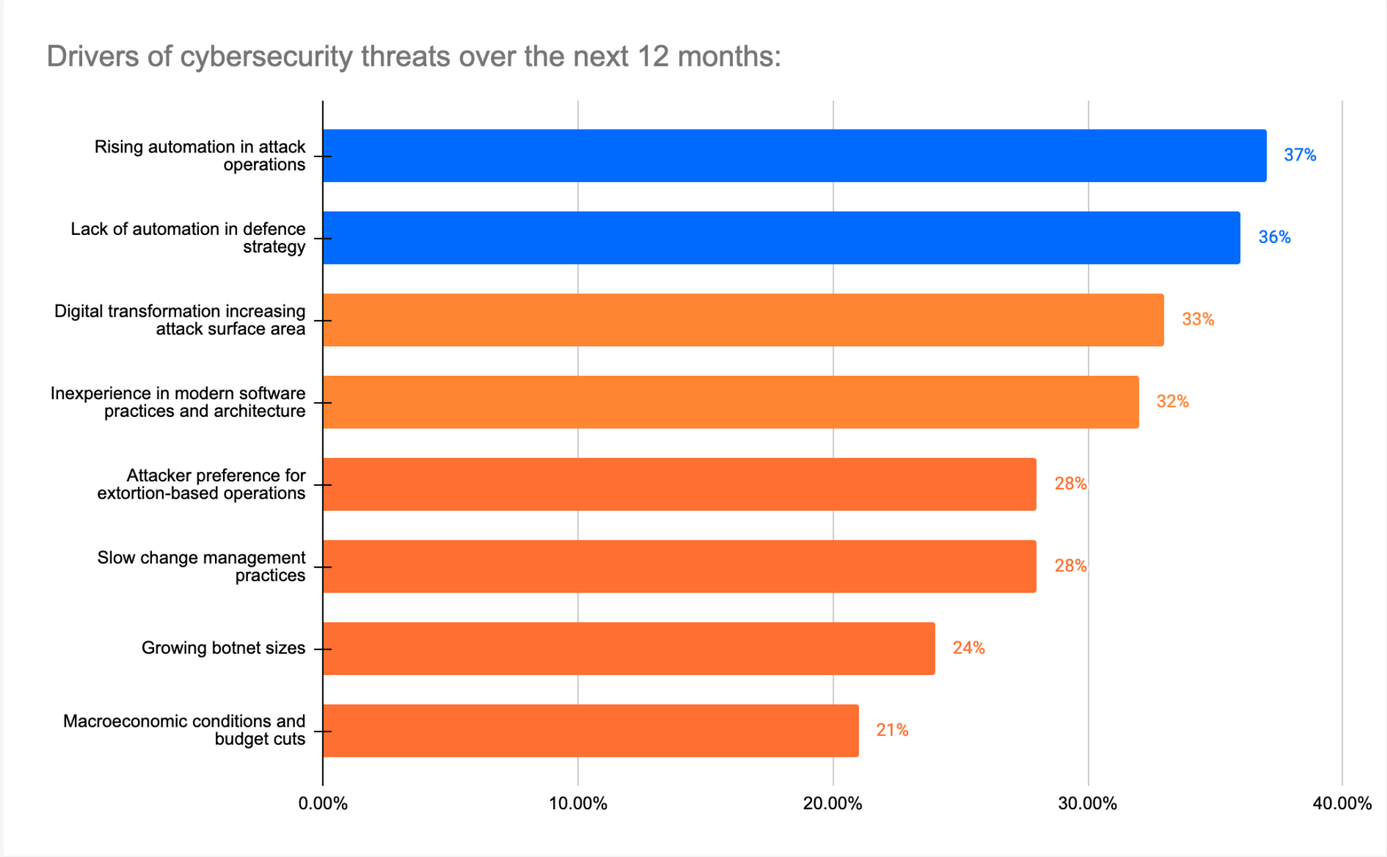
Unternehmen nutzen am häufigsten cloudbasierte DDoS- Schutzservices (81 %) zur Bekämpfung von DDoS-Angriffen.



F1c. Welche Maßnahmen setzt Ihr Unternehmen derzeit zum Schutz vor DDoS-Angriffen ein? Bitte alle zutreffenden Antworten auswählen I Basis: 53 * Es wurden nur diejenigen befragt, die glauben, dass DDoS-Angriffe eine Bedrohung darstellen.

Treibende Kräfte hinter zukünftigen Cybersicherheitsbedrohungen

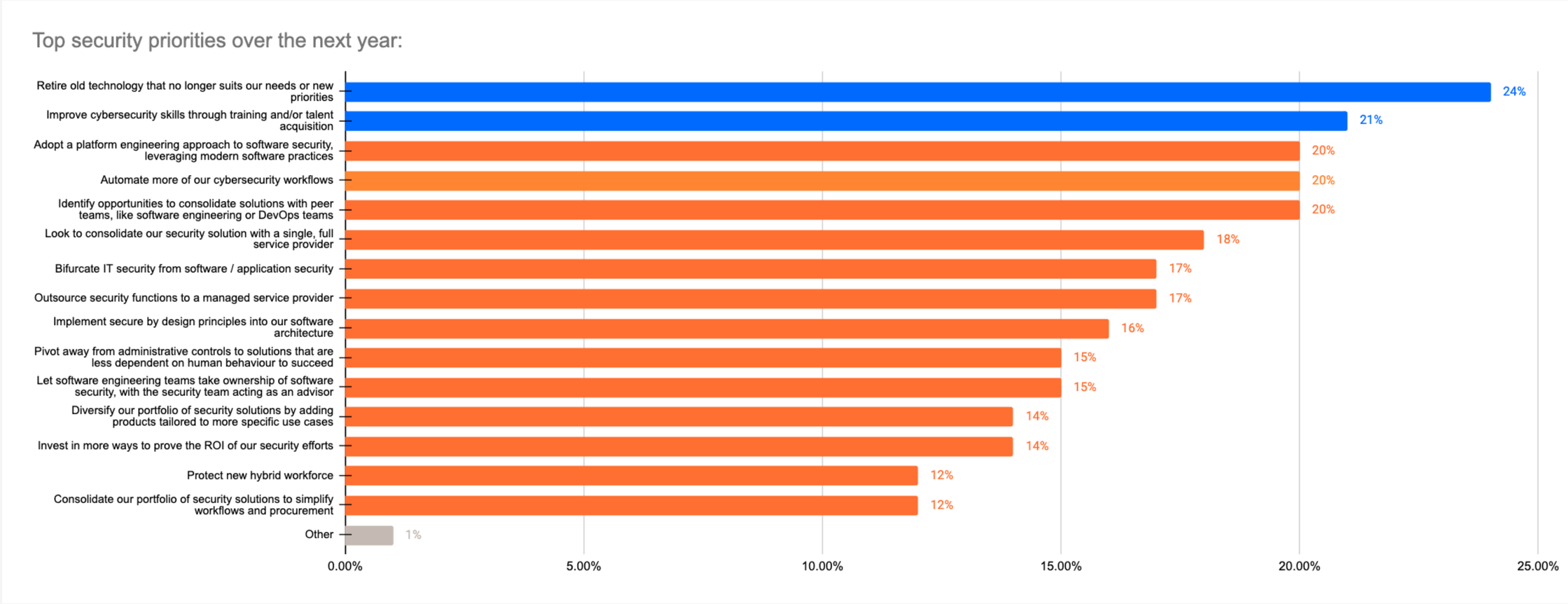
Mit Blick auf die Zukunft glauben Entscheider, dass die zunehmende Automatisierung von Angriffen (37 %) und die fehlende Automatisierung ihrer Verteidigungsstrategie (36 %) die wichtigsten treibenden Kräfte hinter Cybersicherheitsbedrohungen sein werden.



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: 200

Sicherheitsprioritäten für das kommende Jahr

Die wichtigsten Sicherheitsprioritäten der Unternehmen für das kommende Jahr betreffen die Verbesserung ihrer Cybersicherheitskompetenzen (21 %) und den Austausch veralteter Technologien (24 %).



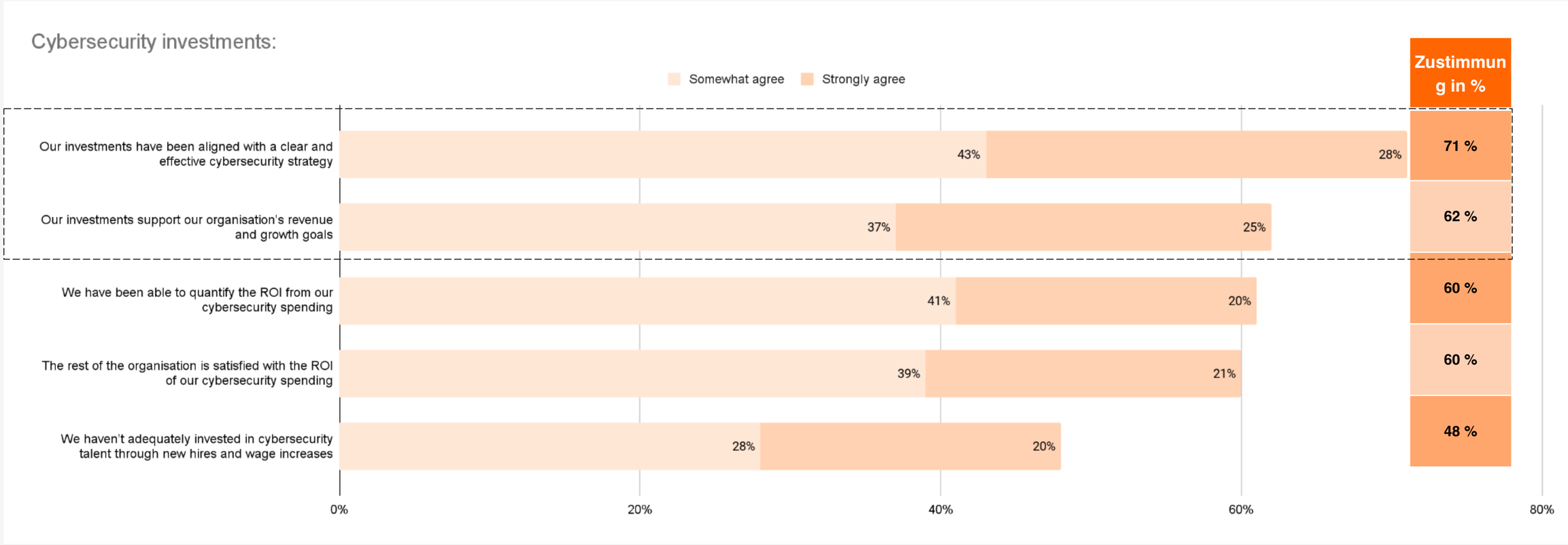
F14. Welche Prioritäten setzt Ihr Unternehmen in puncto Security für das kommende Jahr? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 200

Wichtigste Ergebnisse

Kommen die Ausgaben für die Cybersicherheit zu kurz?

Investitionen in die Cybersicherheit

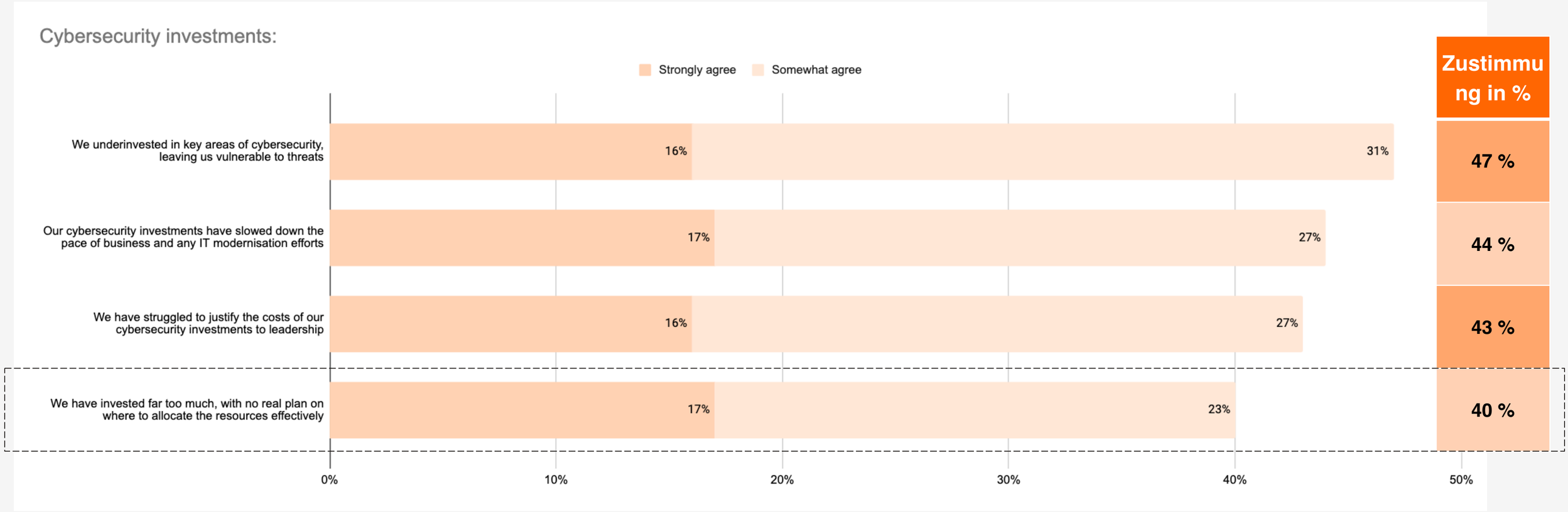
62 % sind der Meinung, dass ihre Investitionen in die Cybersicherheit die Umsatz- und Wachstumsziele ihres Unternehmens unterstützen, und weitere 71 % sind der Ansicht, dass diese Investitionen auf eine klare und effektive Cybersicherheitsstrategie ausgerichtet sind.



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: 200

Investitionen in die Cybersicherheit

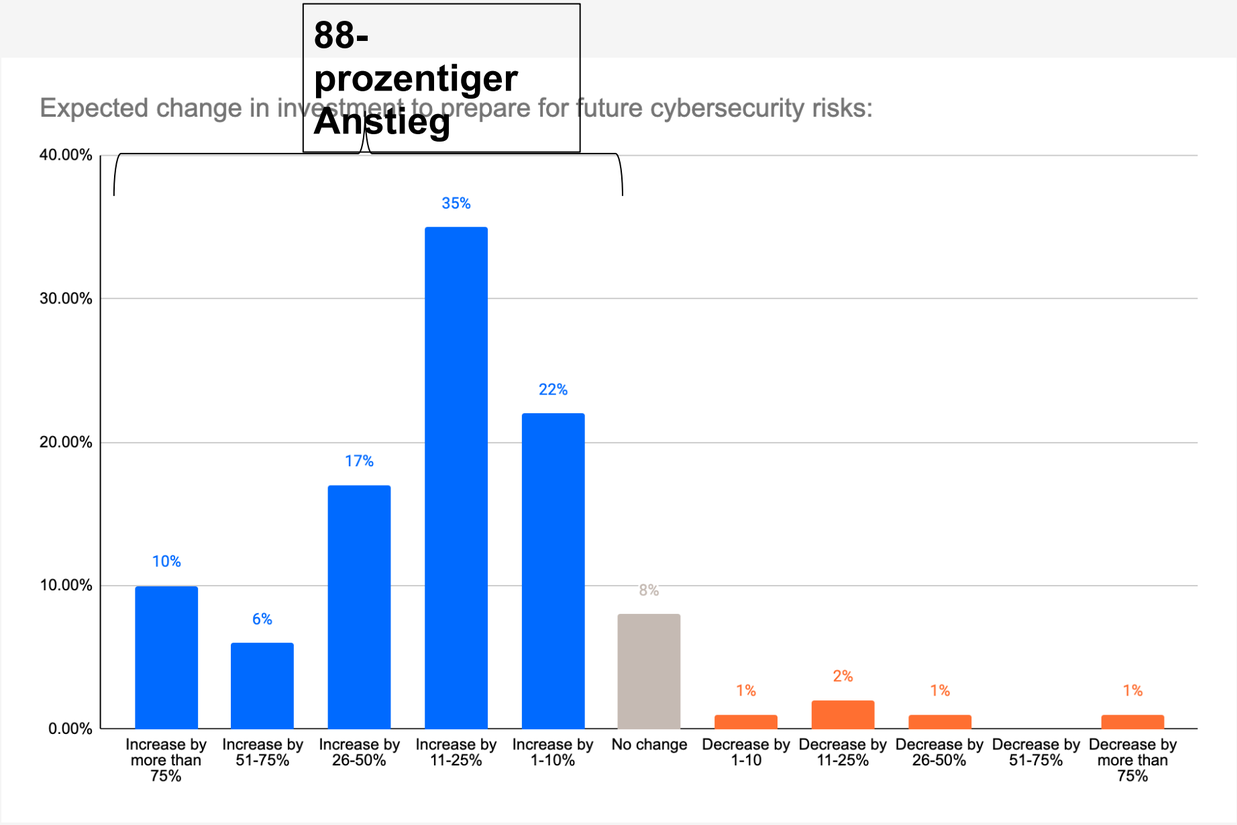
Außerdem stimmen nur 40 % zu, dass sie zu viel investiert haben, ohne einen wirklichen Plan zu haben, wie sie die Ressourcen effektiv einsetzen können. Dies zeigt, dass sich Unternehmen aktiv auf zukünftige Cybersicherheitsrisiken vorbereiten.



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: 200

Änderungen bei künftigen Investitionen in die Cybersicherheit

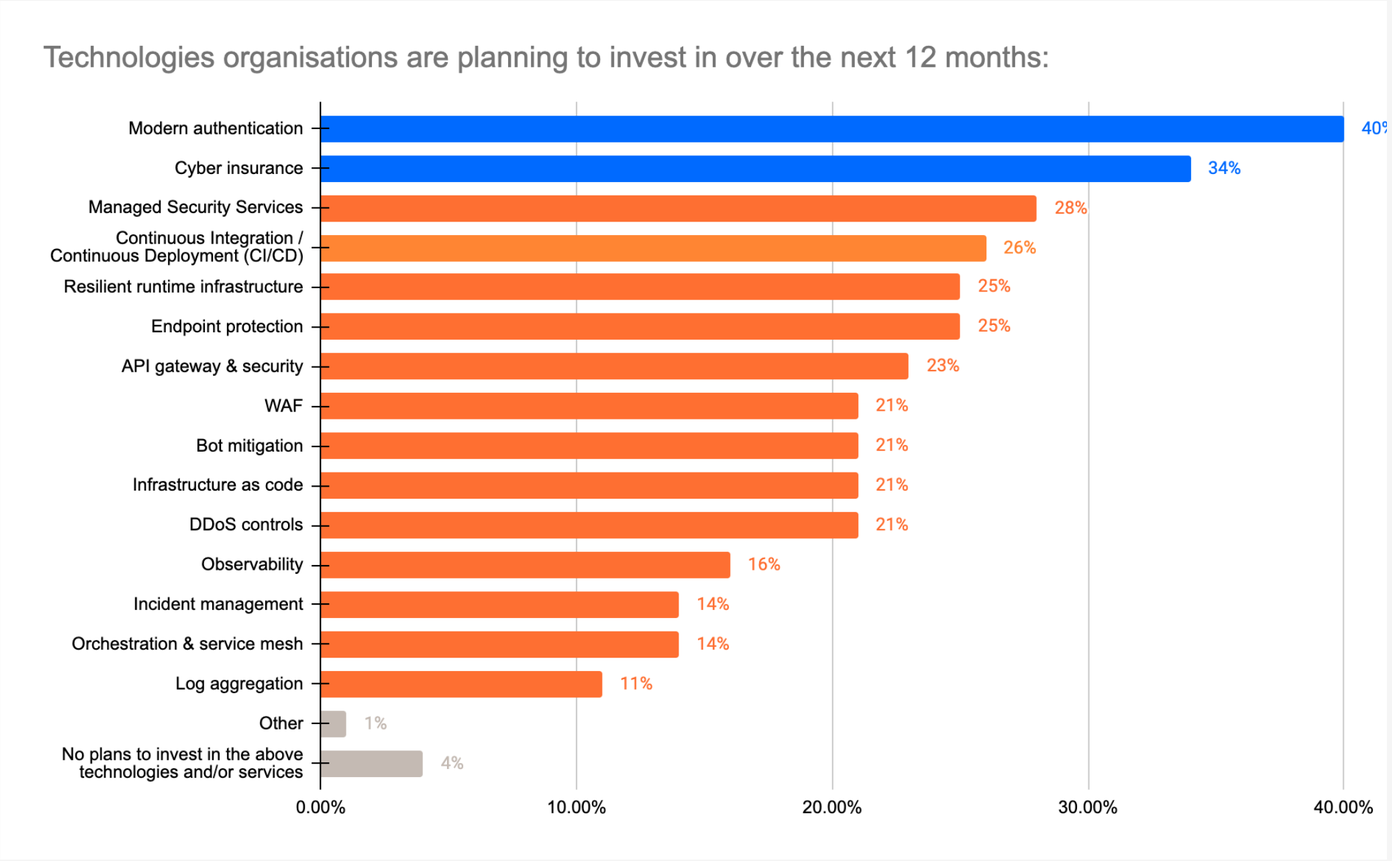
88 % der Entscheider erwarten, dass die Investitionen ihres Unternehmens im Hinblick auf die Vorbereitung auf künftige Cybersicherheitsrisiken in den nächsten 12 Monaten steigen werden.



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: 200

Geplante Investitionen in Cybersicherheitstechnologien

Fast alle Unternehmen planen, in den nächsten 12 Monaten in Technologien zu investieren, insbesondere in moderne Authentifizierung (40 %) und Cyberversicherungen (34 %).



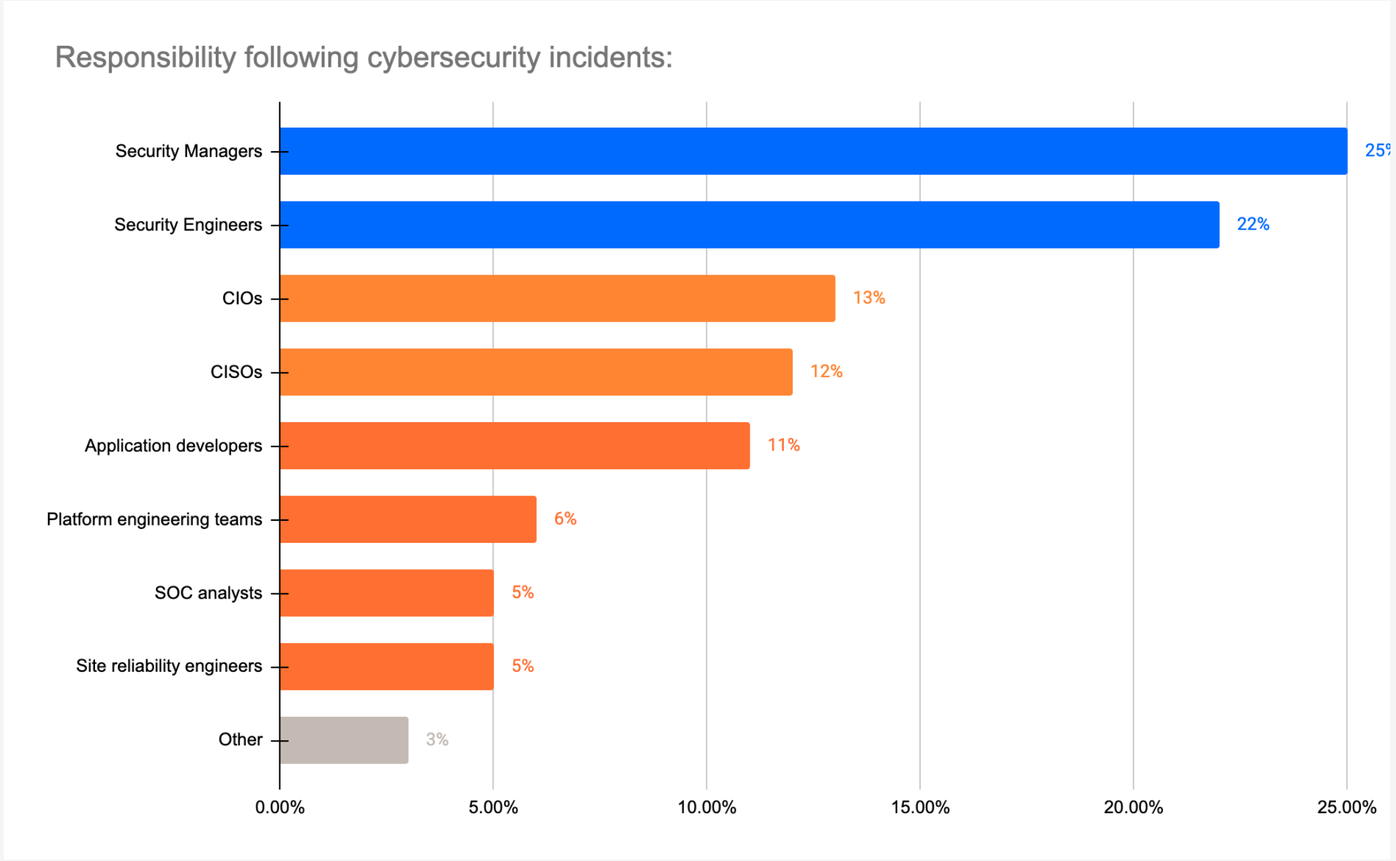
F4. In welche Technologien bzw. Services plant Ihr Unternehmen in den nächsten 12 Monaten zu investieren? Bitte alle zutreffenden Antworten auswählen I Basis: 200

Wichtigste Ergebnisse

Verschiebungen der Zuständigkeiten

Verantwortung für Cybersicherheitsvorfälle

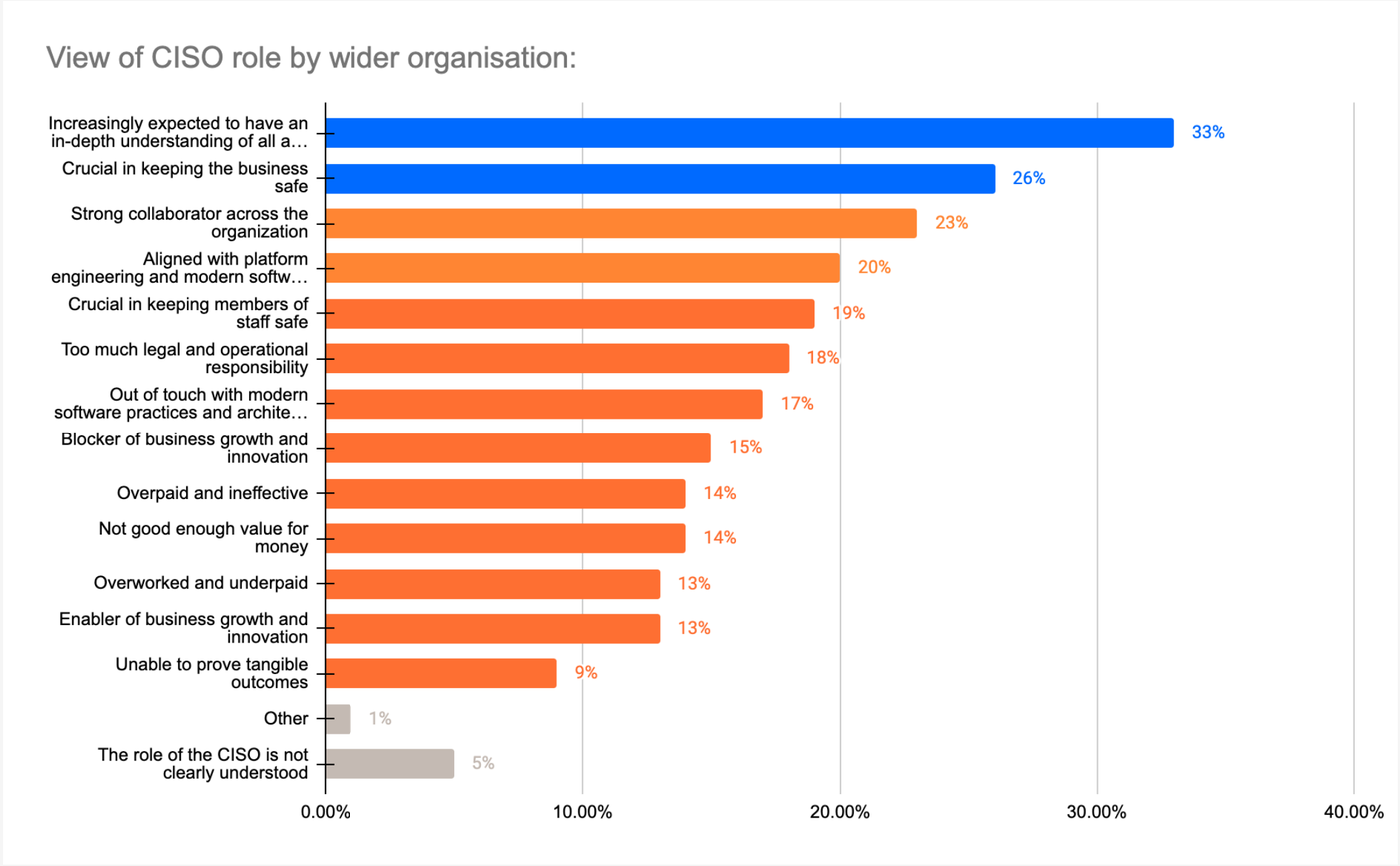
Die Personenkreise, die für Sicherheitsvorfälle zur Verantwortung gezogen werden, sind breit gestreut. Am häufigsten tragen allerdings Security Manager (25 %) und Entwickler (22 %) die Verantwortung für Cybersicherheitsvorfälle.



F9. Wer wird Ihrer Meinung nach am häufigsten für Cybersicherheitsvorfälle in Ihrem Unternehmen zur Verantwortung gezogen? Bitte eine Antwort auswählen I Basis: 200

Wahrnehmung der CISO-Rolle

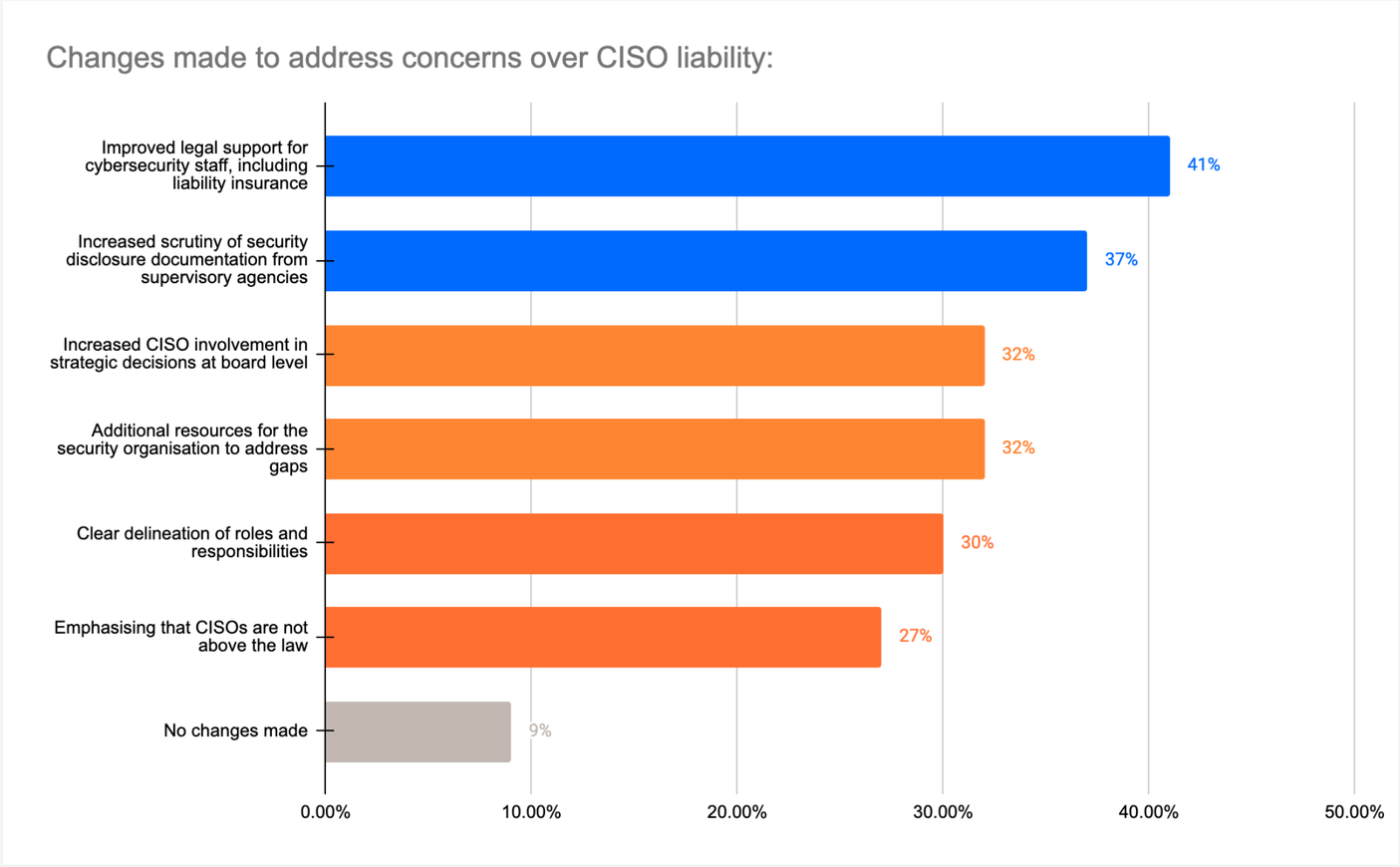
Entscheider sind der Ansicht, dass von CISOs zunehmend erwartet wird, dass sie über ein tiefgreifendes Verständnis aller IT-Bereiche verfügen (33 %), und dass sie als entscheidend für die Sicherheit des Unternehmens gelten (26 %).



F10. Wie wird die Rolle des CISO Ihrer Meinung nach in Ihrem Unternehmen wahrgenommen? Bitte die drei am ehesten zutreffenden Antworten auswählen I Basis: 200

Änderungen, die die Verantwortlichkeiten von CISOs betreffen

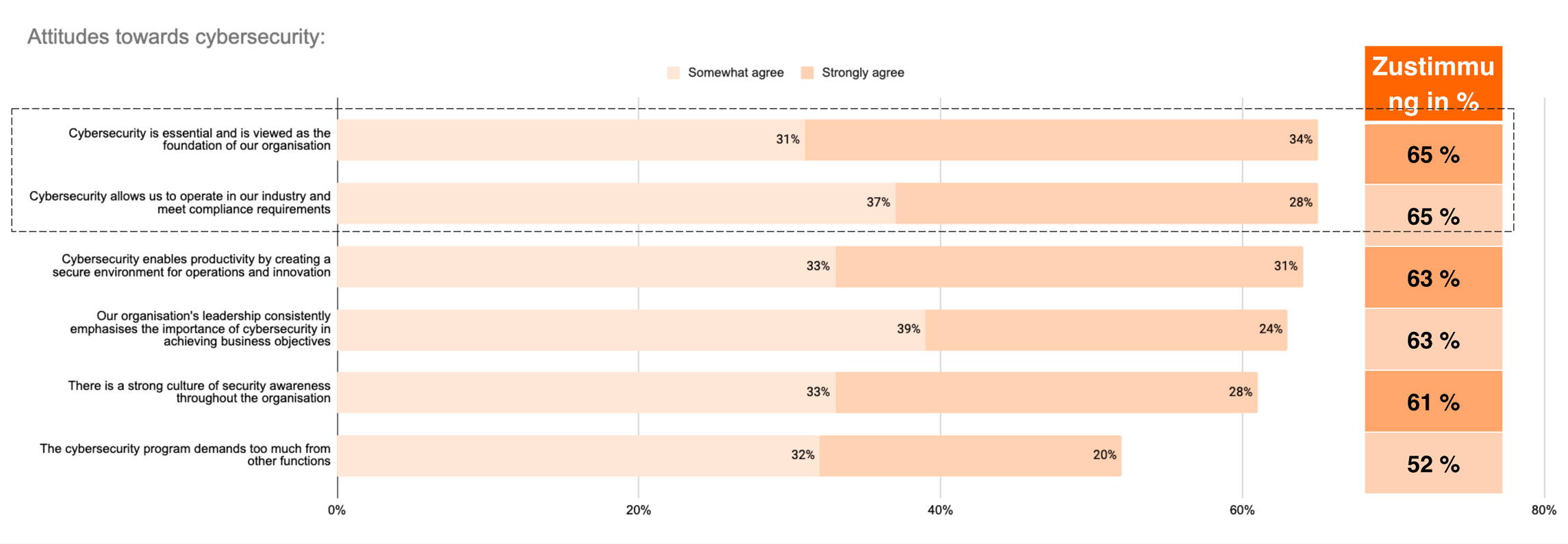
Entscheider sind der Ansicht, dass von CISOs zunehmend erwartet wird, dass sie über ein tiefgreifendes Verständnis aller IT-Bereiche verfügen (33 %), und dass sie als entscheidend für die Sicherheit des Unternehmens gelten (26 %).



F12. Welche Änderungen hat Ihr Unternehmen hinsichtlich der Verantwortlichkeiten von CISOs bereits umgesetzt? Bitte alle zutreffenden Antworten auswählen I Basis: 200

Wahrgenommener Stellenwert von Cybersicherheit

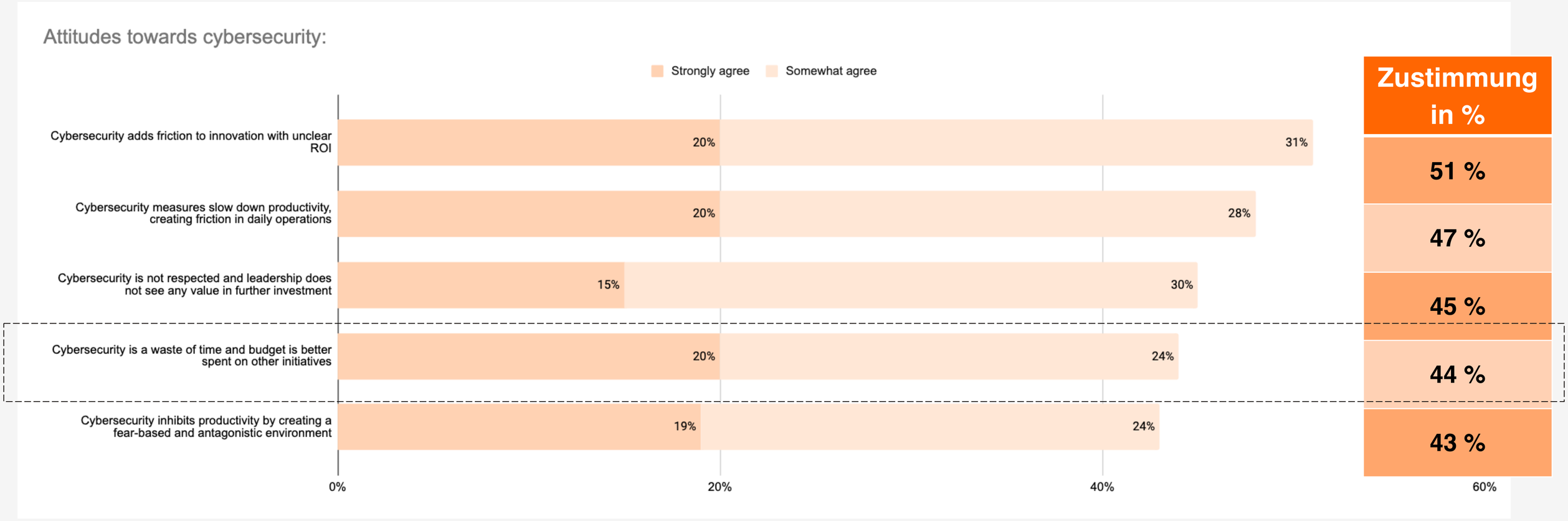
Es herrscht ein starker Konsens darüber, dass Cybersicherheit unverzichtbar ist, insbesondere wenn es um die Erfüllung von Compliance-Anforderungen geht (je 65 %).



F11. Denken Sie an den wahrgenommenen Stellenwert der Cybersicherheit in Ihrem Unternehmen. Inwieweit stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 200

Wahrgenommener Stellenwert von Cybersicherheit

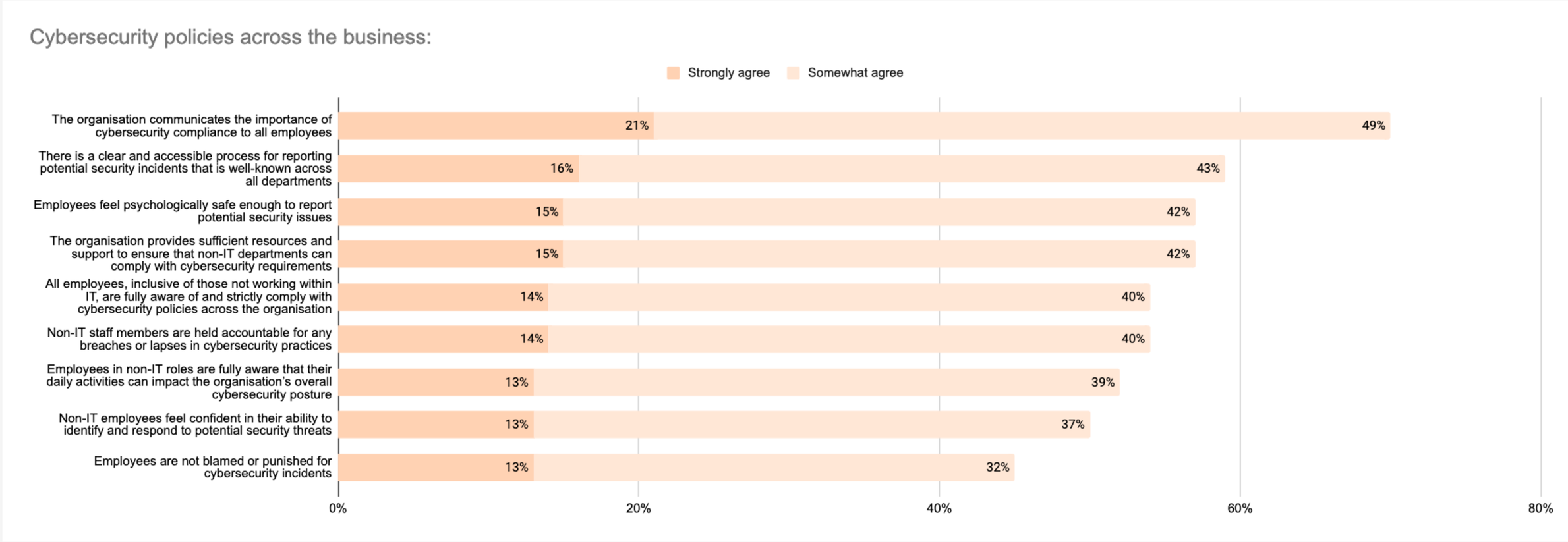
Nur 44 % der Befragten sind der Meinung, dass Cybersicherheit eine Zeitverschwendung ist und dass das Budget besser an anderer Stelle eingesetzt werden sollte.



F11. Denken Sie an den wahrgenommenen Stellenwert der Cybersicherheit in Ihrem Unternehmen. Inwieweit stimmen Sie den folgenden Aussagen zu oder nicht zu? I Basis: 200

Cybersicherheitsrichtlinien

In 59 % der Unternehmen herrscht eine ausgeprägte abteilungsübergreifende Compliance-Kultur, was Richtlinien für die Cybersicherheit betrifft. Diese wird durch eine effektive Kommunikation über die Bedeutung von Sicherheit unterstützt (69 %).



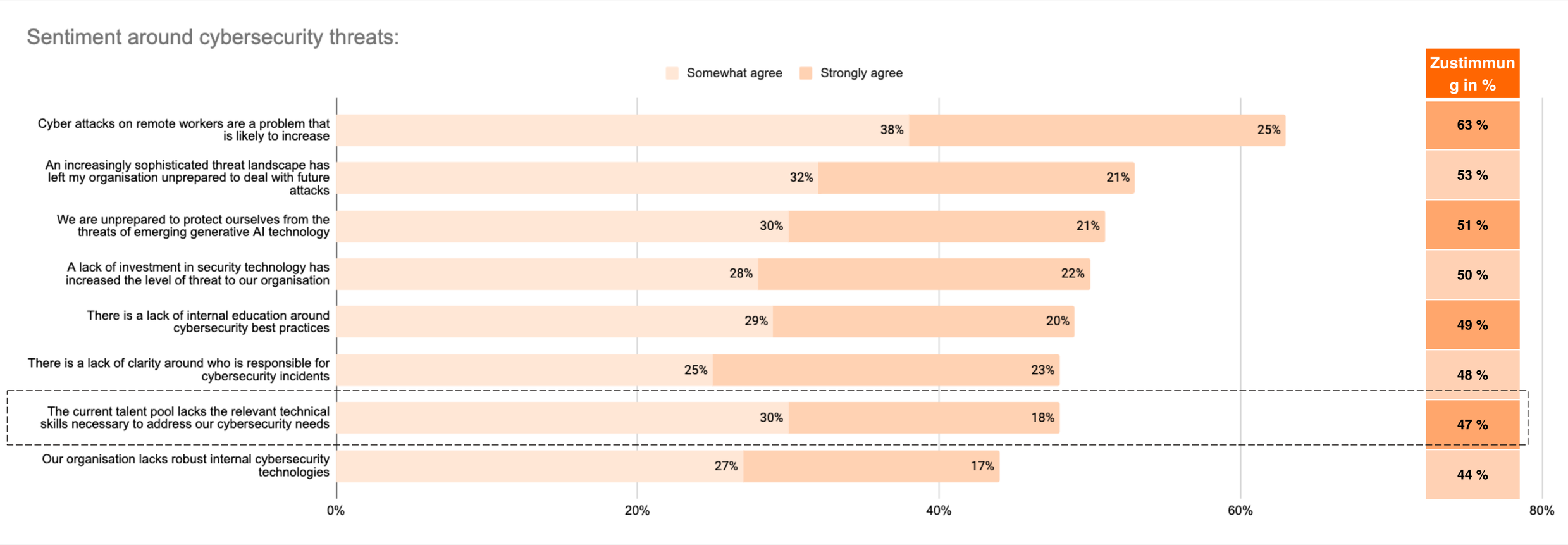
F13. Denken Sie darüber nach, wie gut die Cybersicherheitsrichtlinien in Ihrem Unternehmen von allen Beschäftigten befolgt werden – Nicht-IT-Abteilungen eingeschlossen. Inwieweit stimmen Sie den folgenden Aussagen zu? I Basis: 200

Wichtigste Ergebnisse

Talentpool im Bereich Cybersicherheit

Cybersicherheitsrisiken

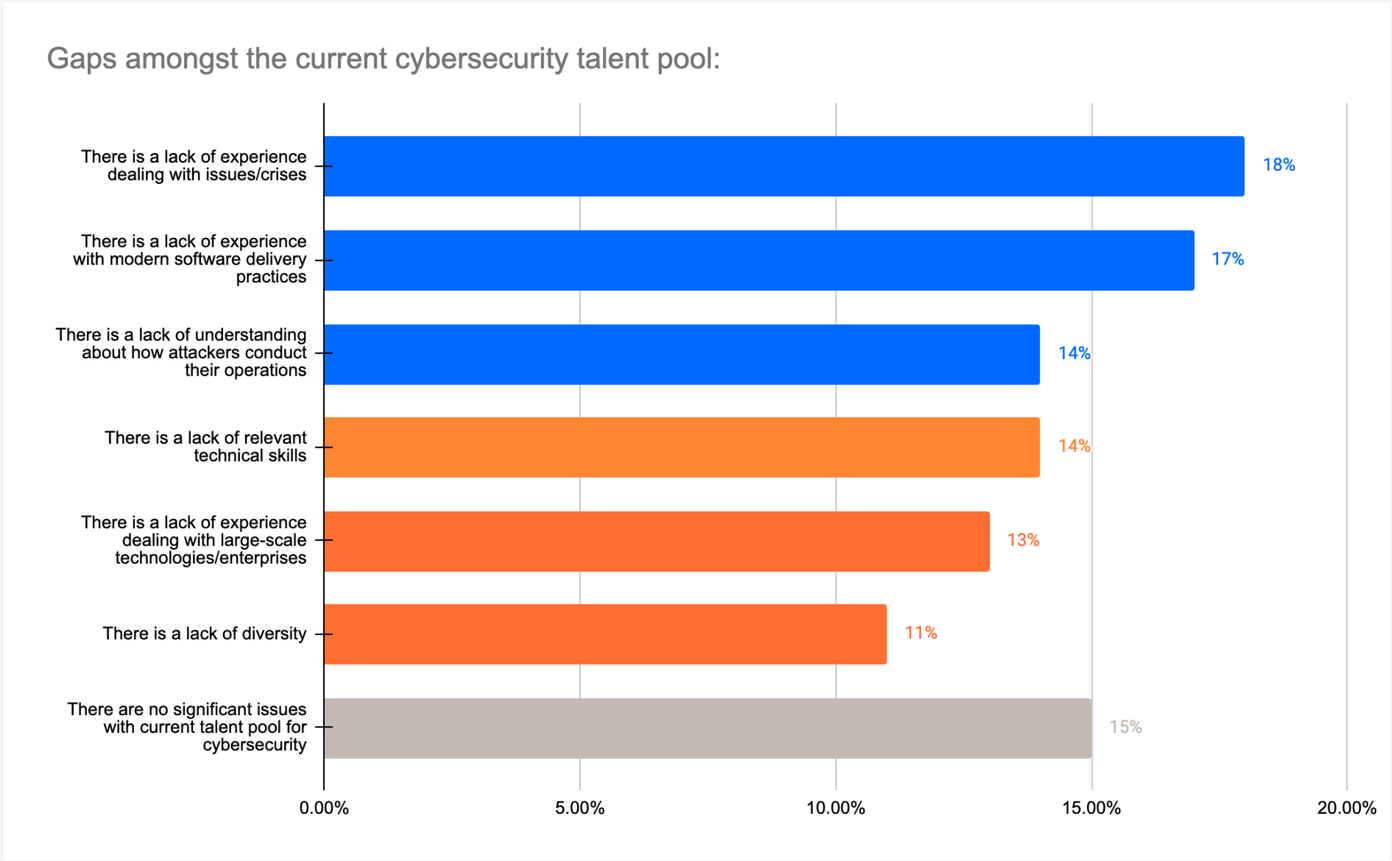
Die Besorgnis über Cyberangriffe auf Remote-Mitarbeiter steigt (63 %), da Unternehmen darauf möglicherweise nicht vorbereitet sind. 47 % der Entscheider im Bereich Cybersicherheit sind der Meinung, dass derzeit ein Mangel an Fachkräften herrscht, die ihre Anforderungen erfüllen.



F2. Inwieweit stimmen Sie den folgenden Aussagen über Bedrohungen der Cybersicherheit in Ihrem Unternehmen zu? I Basis: 200

Fachkräftemangel im Bereich Cybersicherheit

Allgemein betrachtet gibt es vielerlei Gründe für den Fachkräftemangel, wobei sich keine eindeutige Ursache dafür ableiten lässt. 86 % bestätigen allerdings, dass es Probleme gibt.



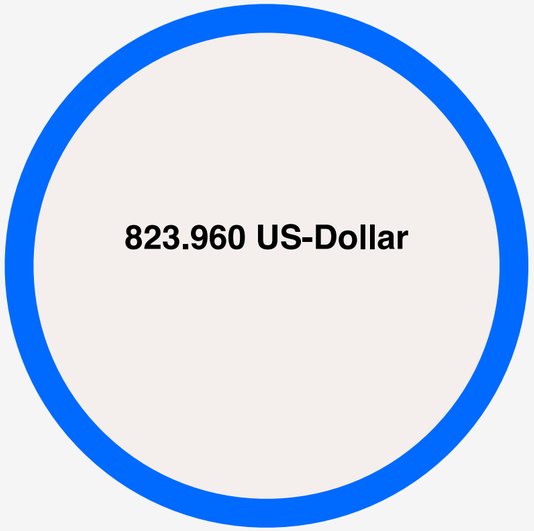
F8. Wo gibt es Ihrer Meinung im derzeitigen Talentpool Nachholbedarf, wenn es um Cybersicherheit geht? Bitte eine Antwort auswählen I Basis: 200

Wichtigste Ergebnisse

Investitionstrends im Bereich Cybersicherheit

Jährliche Ausgaben für die Sicherheit von Webanwendungen und APIs

Im Durchschnitt geben Unternehmen jährlich 823.960 US-Dollar für Sicherheitskontrollen und -Tools für Webanwendungen und APIs aus. Dabei verlassen sie sich im Durchschnitt auf 8 verschiedene Cybersicherheitslösungen.



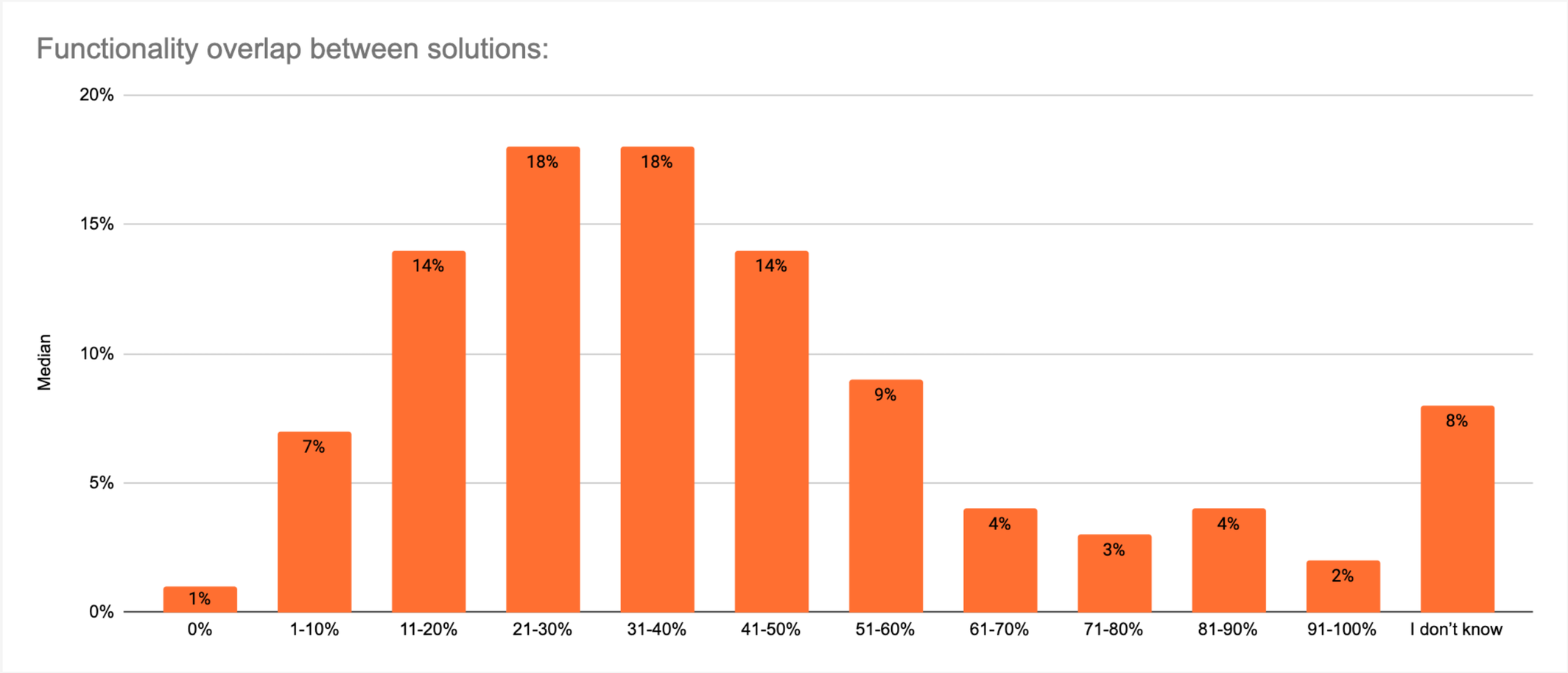
Durchschnittlicher Betrag, der jährlich für Webanwendungs- und API-Sicherheitskontrollen/-Tools ausgegeben wird

Durchschnittliche Zahl der Cybersicherheitslösungen für Netzwerke und Anwendungen, auf die sich Unternehmen verlassen

F7a. Wie hoch schätzen Sie die jährlichen Ausgaben (in US-Dollar) Ihres Unternehmens für Web-App- und API-Sicherheitsmaßnahmen und -tools? I Basis: 200

Überschneidungen bei den Cybersicherheitslösungen

Im Durchschnitt überschneiden sich 38 % dieser Cybersicherheitslösungen in ihrer primären Funktion.



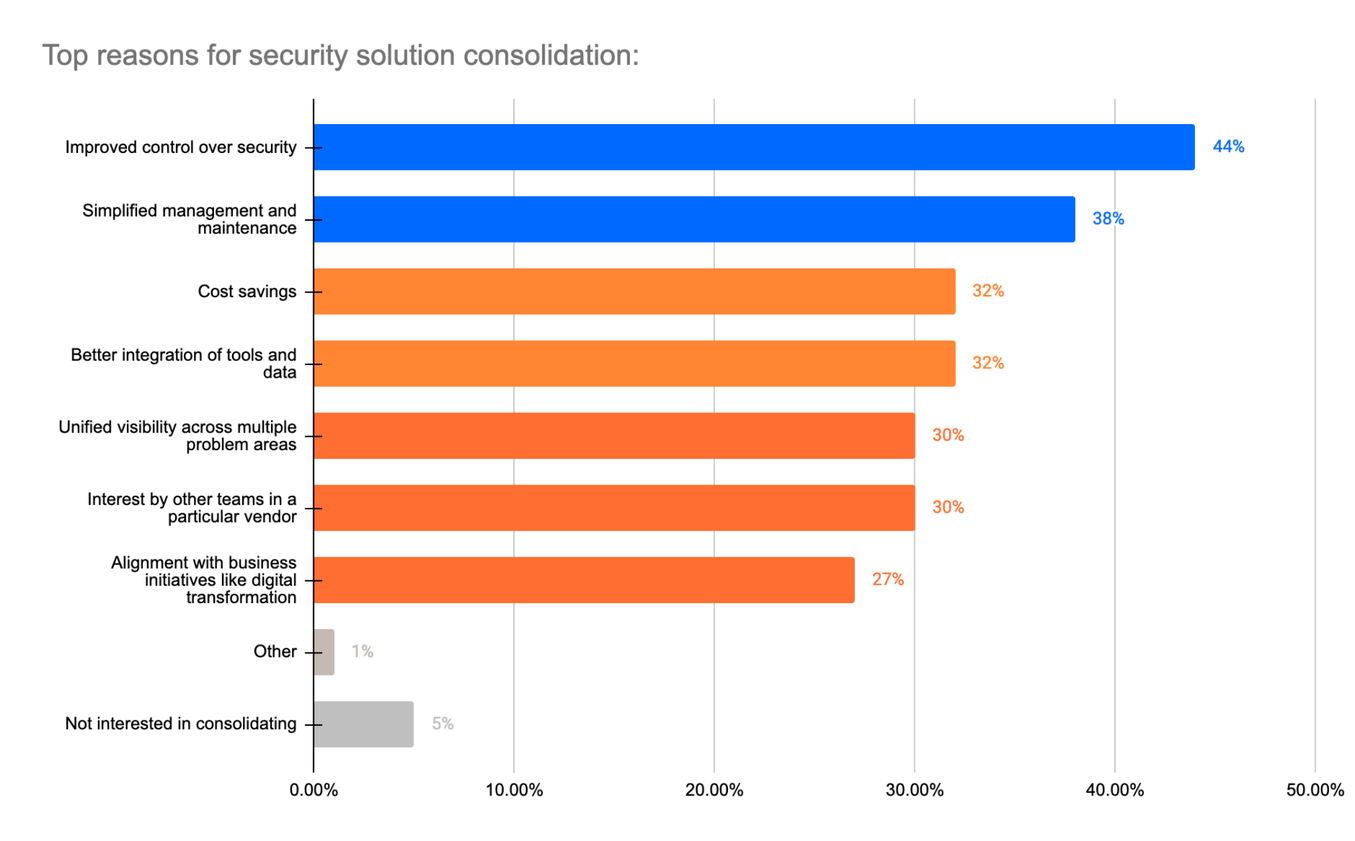
F7c. Wie viele dieser Lösungen überschneiden sich in etwa in ihrer primären Funktion? Bitte eine Antwort auswählen I Basis: 200

Wichtigste Ergebnisse

Konsolidierung und Integration von Sicherheitslösungen

Gründe für die Konsolidierung von Sicherheitslösungen

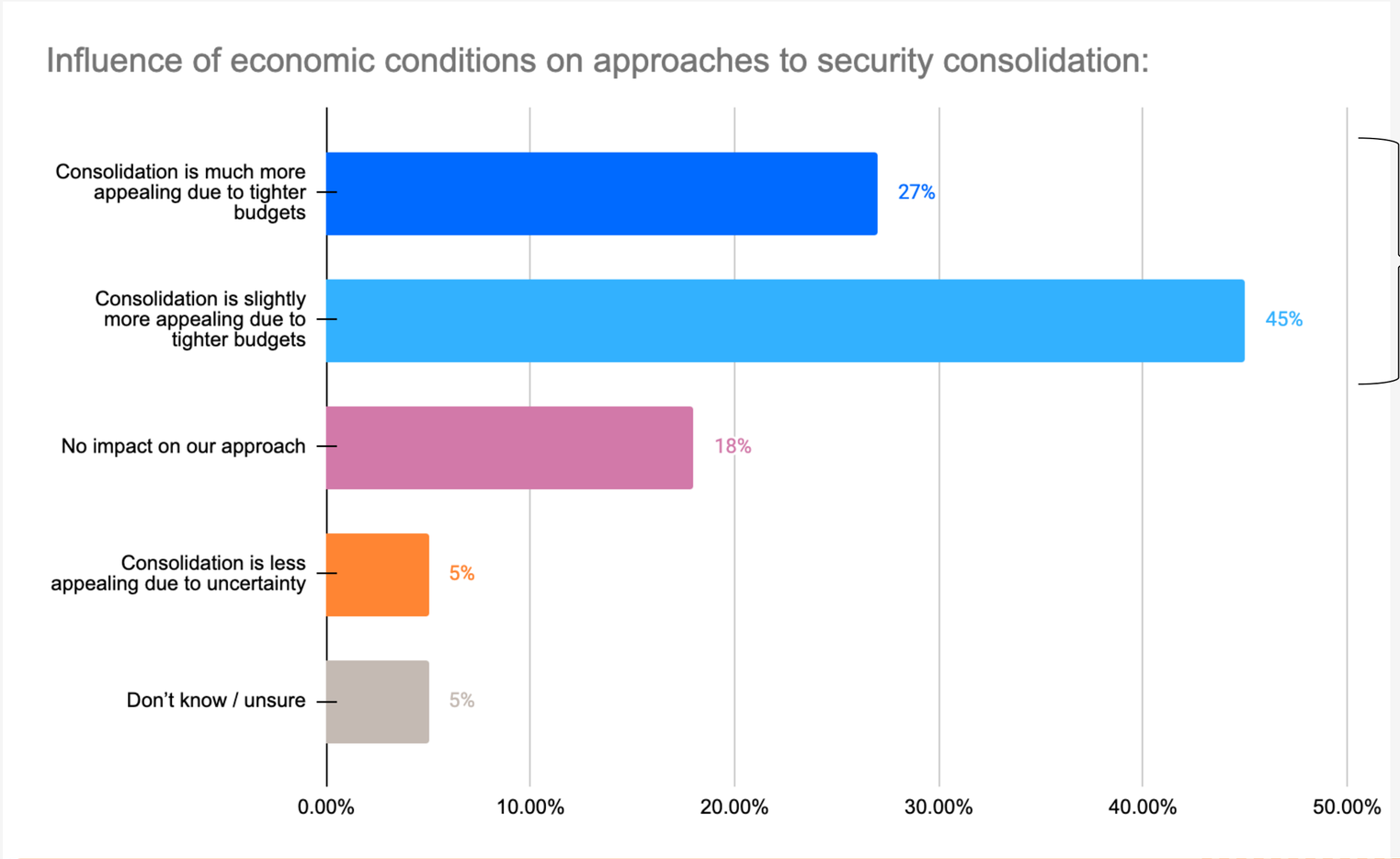
44 % führen das Interesse ihres Unternehmens an der Konsolidierung von Sicherheitslösungen auf eine verbesserte Kontrolle über die Sicherheit zurück, während weitere 38 % die Verwaltung und Wartung vereinfachen wollen.



F23a. Wenn Ihr Unternehmen an einer Konsolidierung von Sicherheitslösungen interessiert ist, was sind die Hauptgründe dafür? Bitte alle zutreffenden Antworten auswählen I Basis: 200

Wirtschaftliche Faktoren für die Konsolidierung von Sicherheitslösungen

72 % der Befragten geben an, dass eine Konsolidierung aufgrund knapperer Budgets interessant sei.

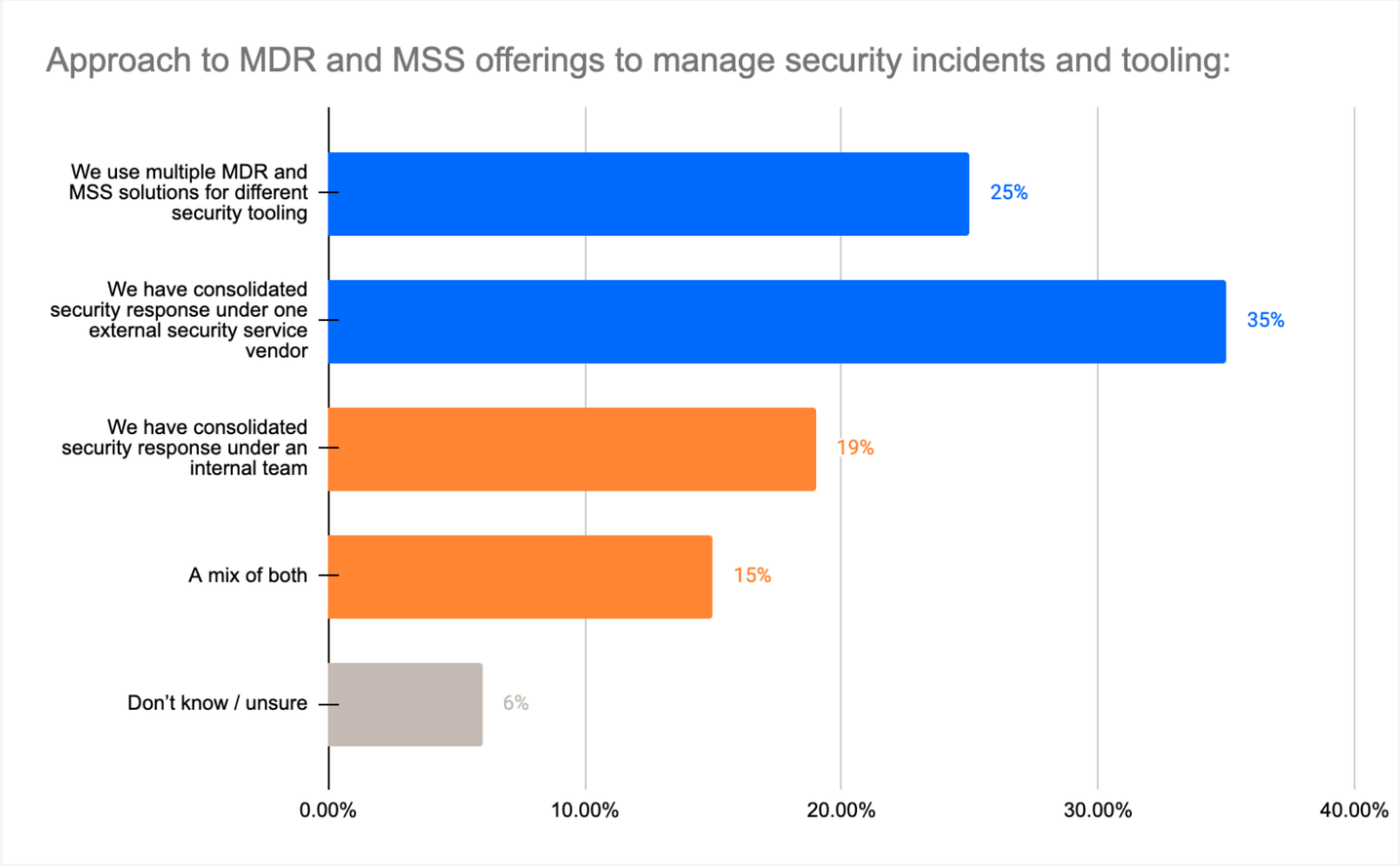


72-prozentige Steigerung des Interesses

F23b. Wie hat sich die Konjunktur auf den Ansatz Ihres Unternehmens bei der Konsolidierung von Sicherheitslösungen ausgewirkt? Bitte eine Antwort auswählen I Basis: 187

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

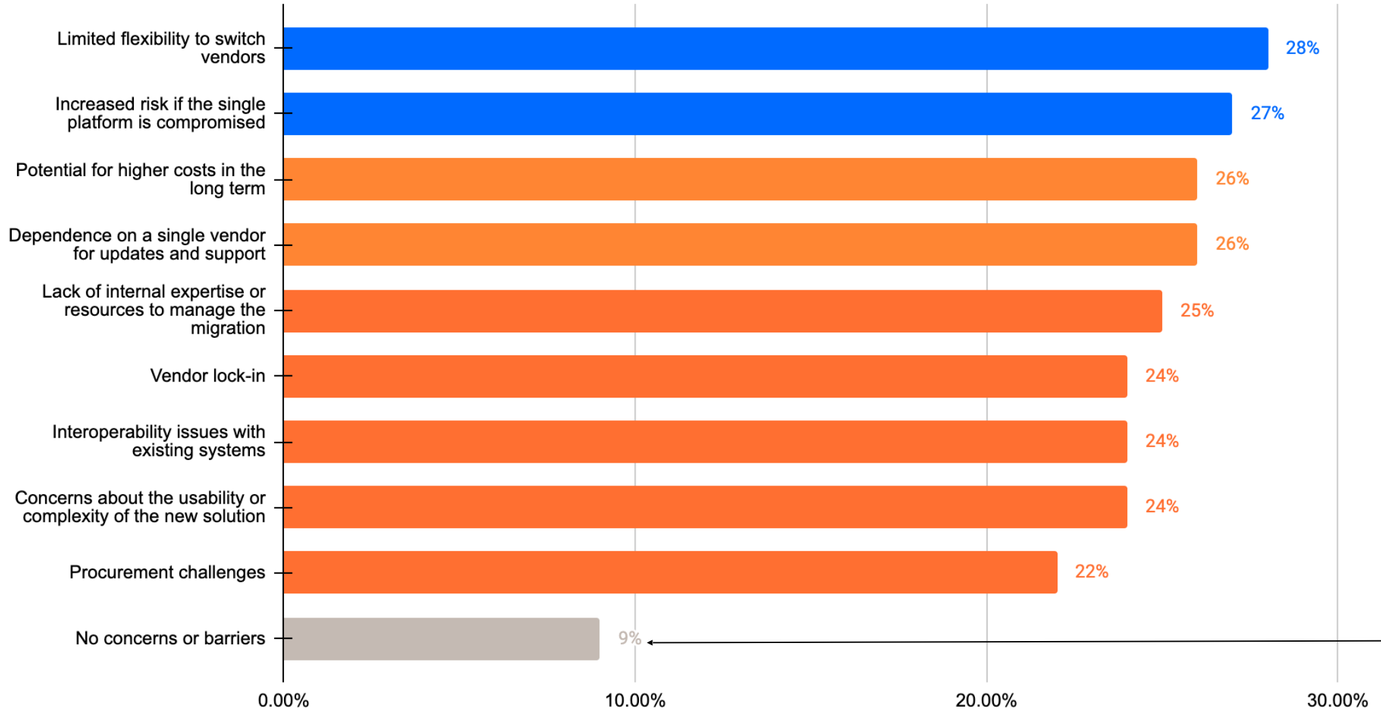
35 % haben ihre Sicherheitsmaßnahmen bei einem externen Serviceanbieter konsolidiert, während 25 % mehrere MDR- und MSS-Lösungen für verschiedene Sicherheitstools nutzen.



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: 200

Bedenken hinsichtlich der Konsolidierung von Sicherheitstools

28 % der Befragten sind besorgt über die eingeschränkte Flexibilität beim Anbieterwechsel und 27 % über das erhöhte Risiko im Falle von Schwachstellen bei der Konsolidierung von Sicherheitstools auf einer einzigen Plattform.

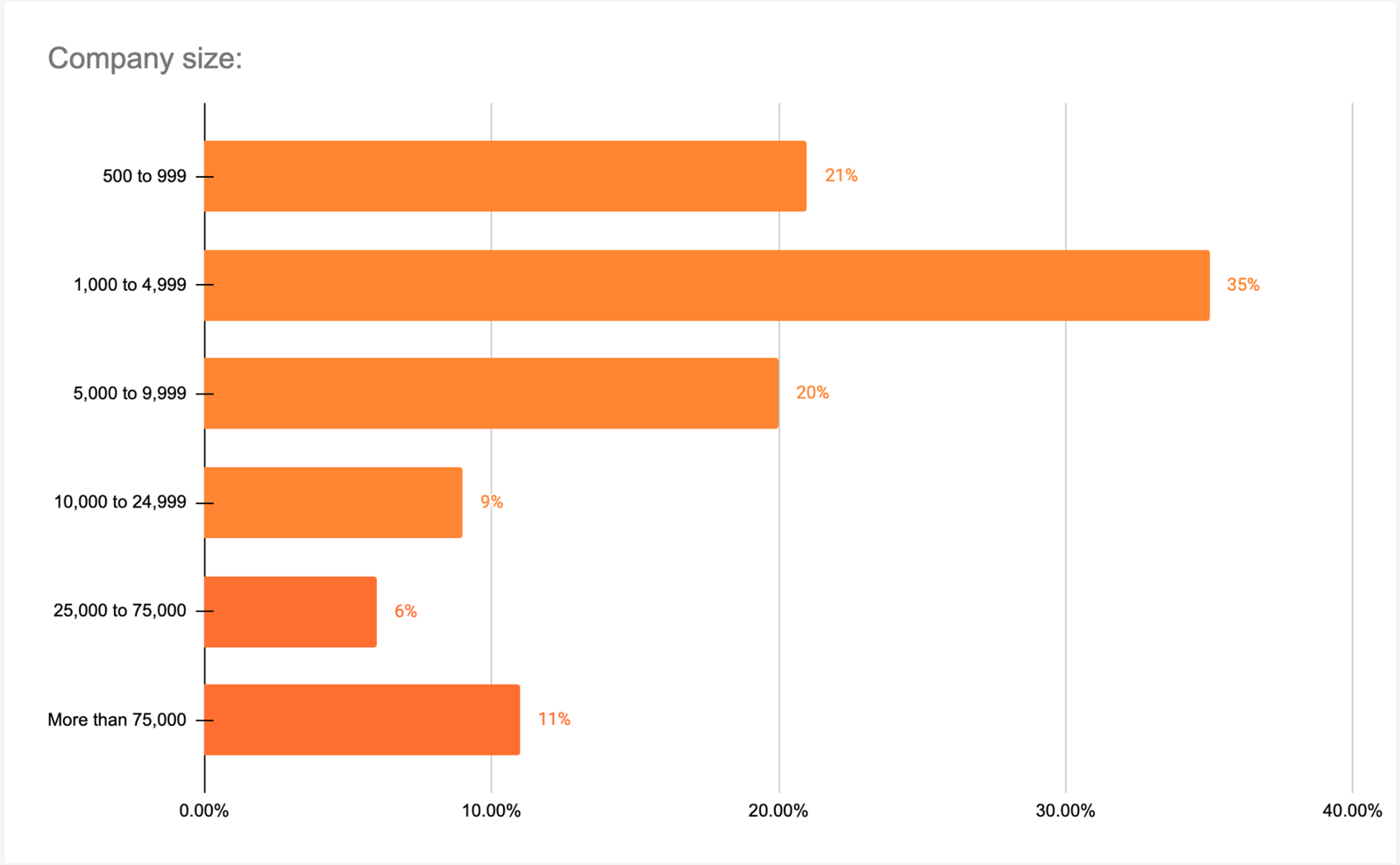


92 % der Unternehmen haben Bedenken oder erkennen Hindernisse, wenn es um die Konsolidierung von Sicherheitstools geht.

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: 200

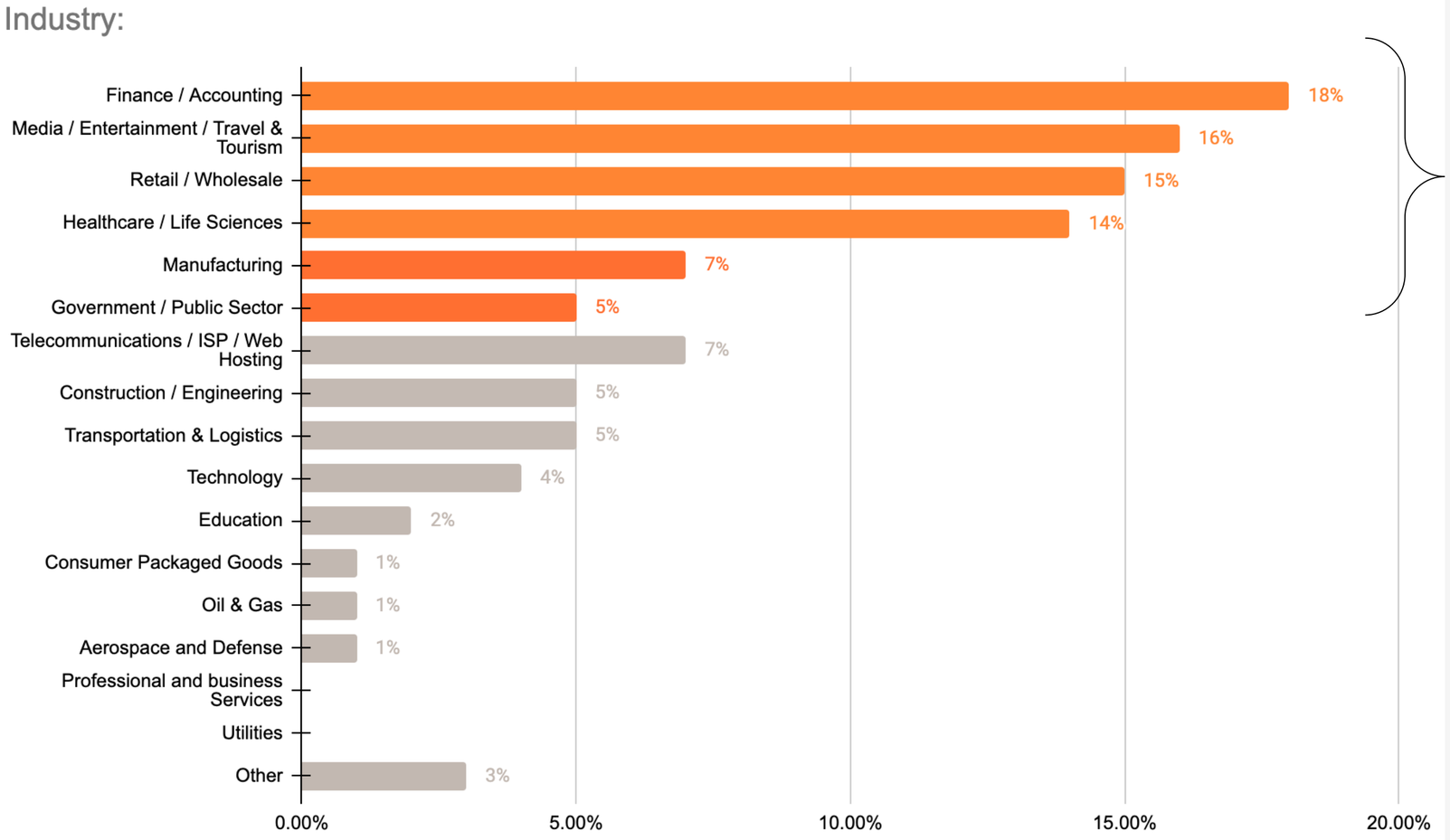
Demografische Daten

Unternehmensgröße



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

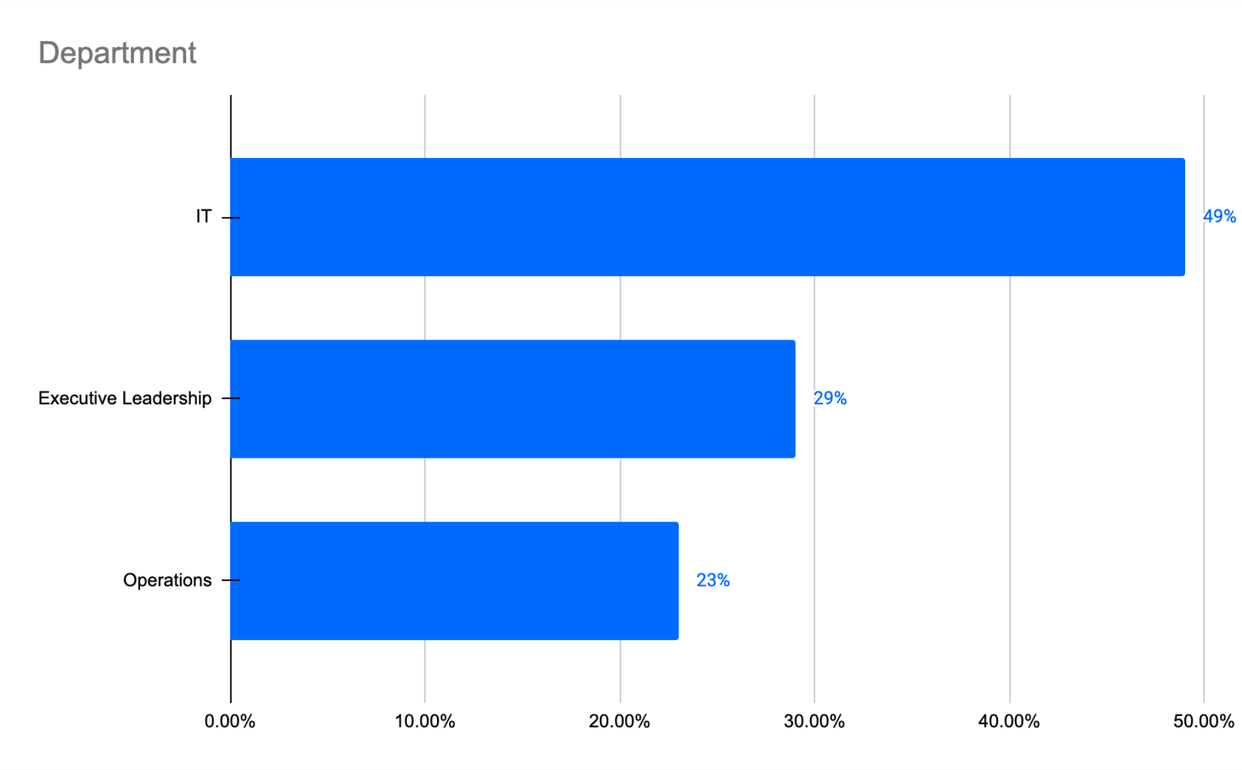
Branche

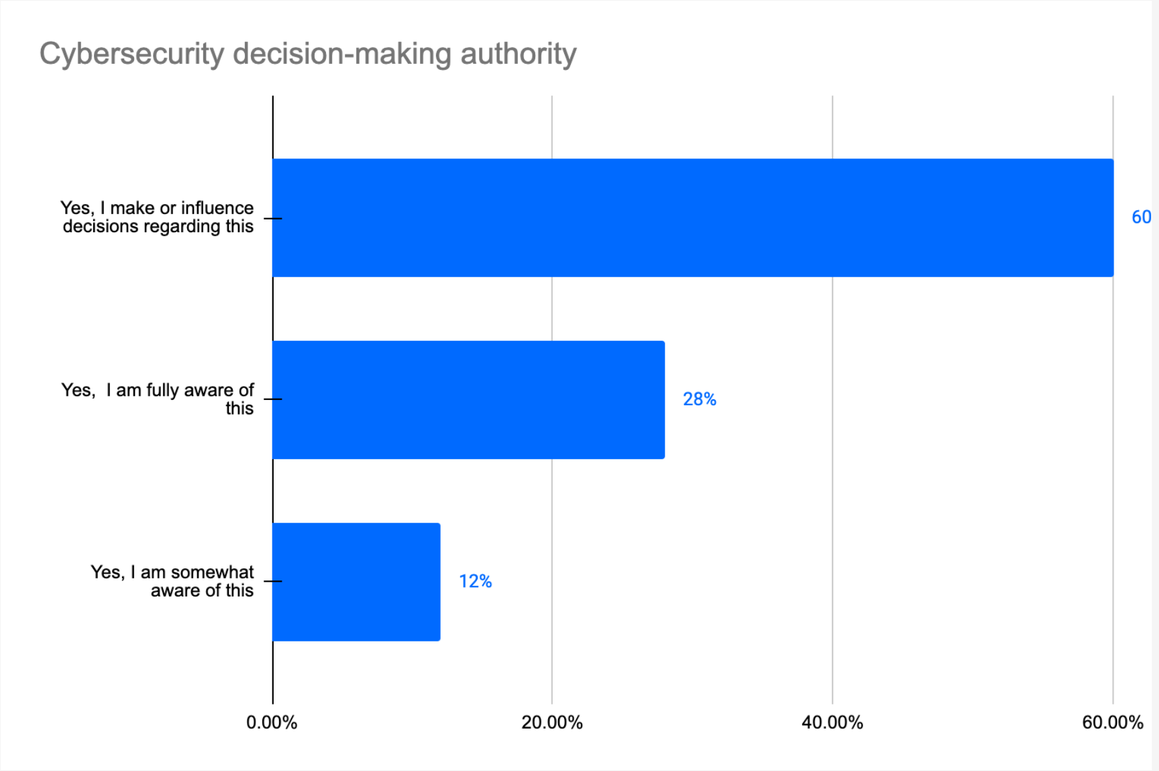


Schwerpunkt-branchen

S3. Welche der folgenden Antworten beschreibt die Branche, in der Ihr Unternehmen tätig ist, am besten? Bitte eine Antwort auswählen I Basis: 200

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: 200

Vielen Dank!