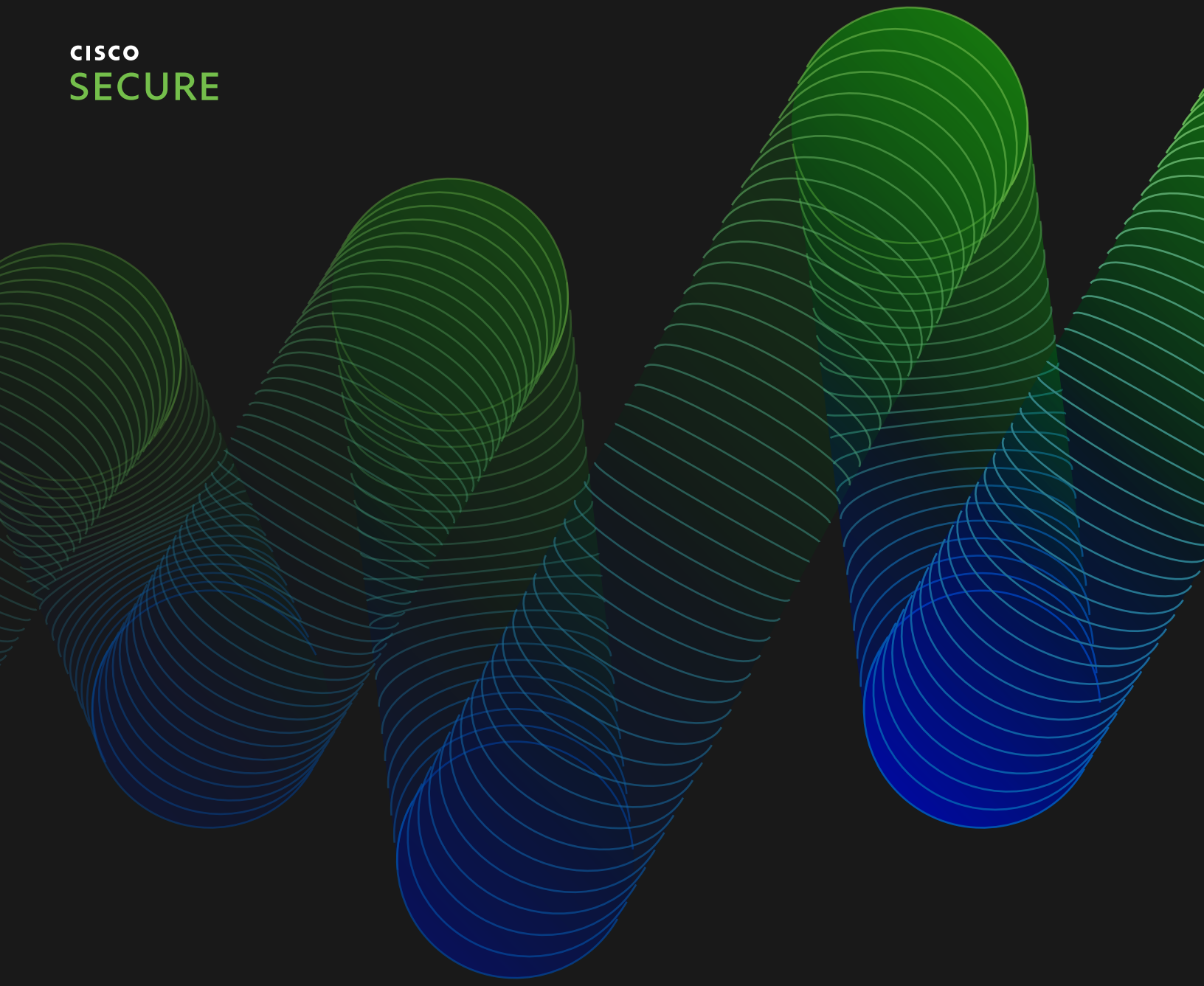
CISCO
SECURE



The State of Security Resilience in LATAM

Findings from the Security Outcomes Report, Volume 3

cisco The bridge to possible

Assessing security resilience

What is security resilience, why is it so important, and how can organizations measurably improve it? Those are the questions we sought to answer in our recently released third volume of the Security Outcomes Report. The report analyzes data collected from over 4,700 security leaders and professionals across the globe. This snapshot focuses on responses from over 1,400 participants working in the Latin America (LATAM) region.

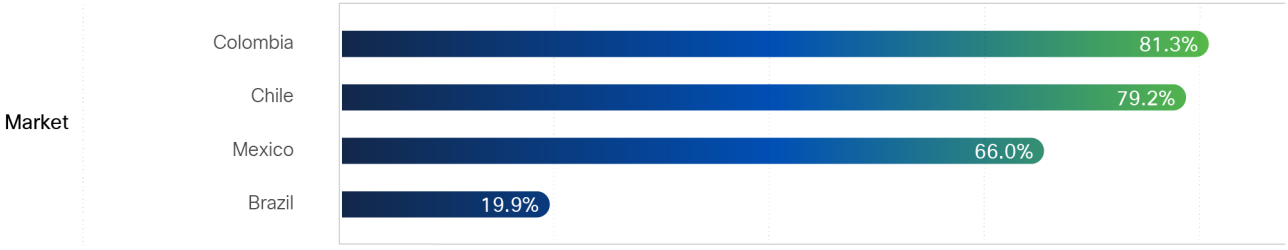
Is resilience on executives' radar?

Yes! We asked respondents about the level of interest and importance top executives place on security resilience. The message couldn't be clearer. A full 96% of LATAM execs consider security resilience highly important, and that statistic varies little across the region.

Do cyber events impact resilience?

Among organizations in LATAM, 60% report experiencing major security incidents that jeopardized business operations, the majority of which occurred in the last few years. (This aligns closely with responses globally, at 62%.) The rate of resilience-impacting events differs dramatically across LATAM. Reported incident frequencies are lowest in Brazil (20% of organizations) and highest in Colombia (81% of organizations), with Chile and Mexico falling toward the upper end of that span.

Figure 1: Rate of reported security incidents that impacted resilience



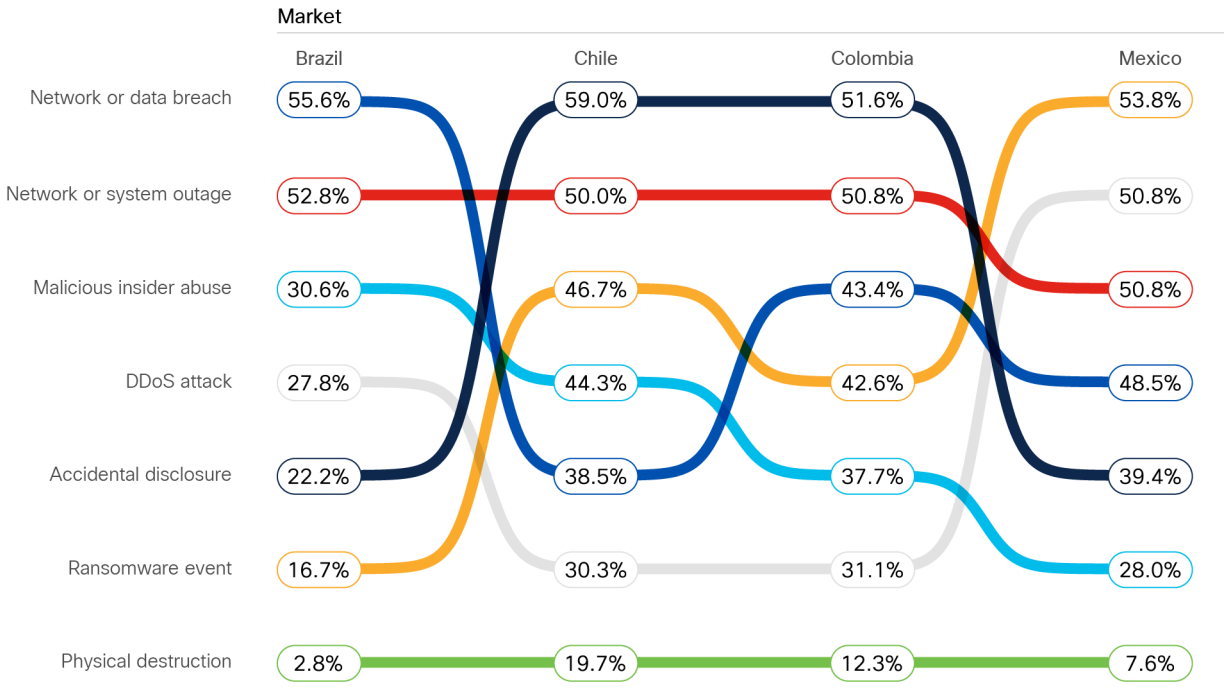
Percentage of organizations that have experienced a security incident

Source: Cisco Security Outcomes Report

What types of cyber events impact resilience?

We asked respondents to elaborate on the types of resilience-impacting incidents they experienced. The chart below ranks common incident types based on the percentage of organizations reporting them in each market. For example, ransomware outbreaks were the most common among firms in Mexico (54%) but ranked next to last in Brazil (17%). Incidents involving physical destruction were the least common in all markets.

Figure 2: Types of security incidents that impacted resilience

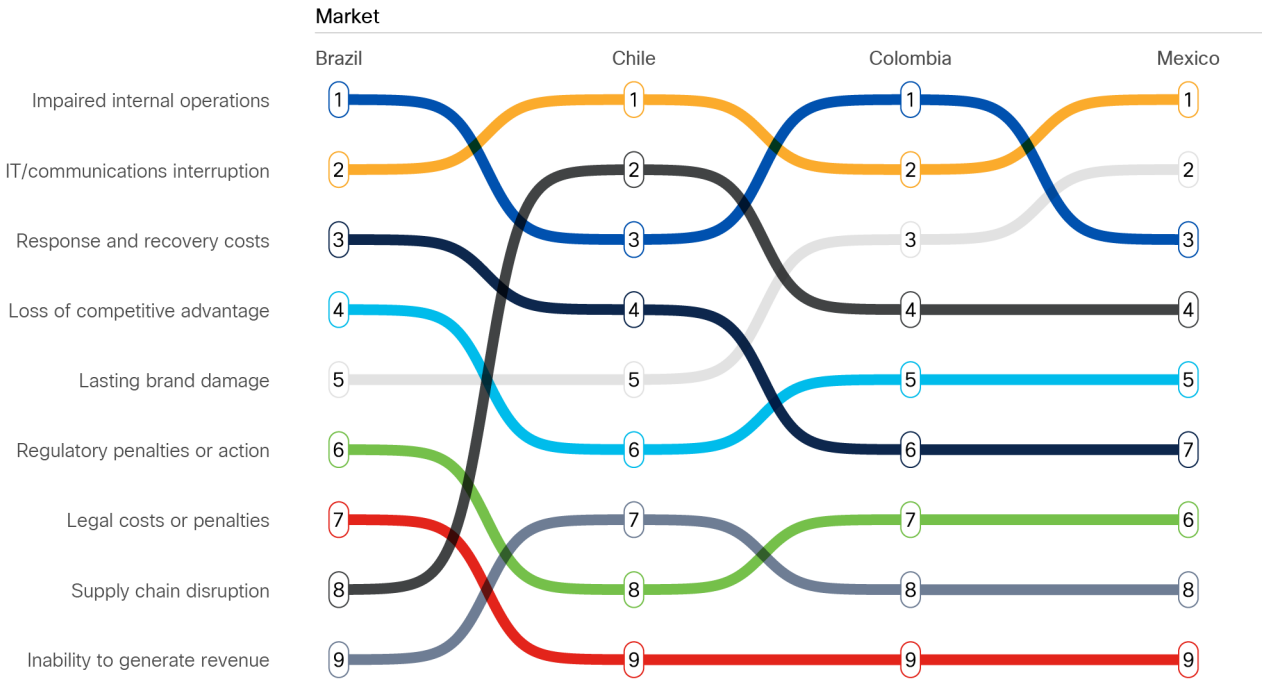


Source: Cisco Security Outcomes Report

What business impacts do incidents cause?

We asked respondents how these major security incidents impacted their organizations. The following chart compares the ranking of impact types based on the percentage of organizations in each LATAM market that reported experiencing them. For example, IT interruptions and impaired internal operations were generally the most common across most markets, while legal costs and inability to generate revenue typically landed at the bottom. Supply chain disruptions in the wake of an incident varied from #2 in Chile to #9 in Brazil.

Figure 3: Types of resilience impacts caused by security incidents



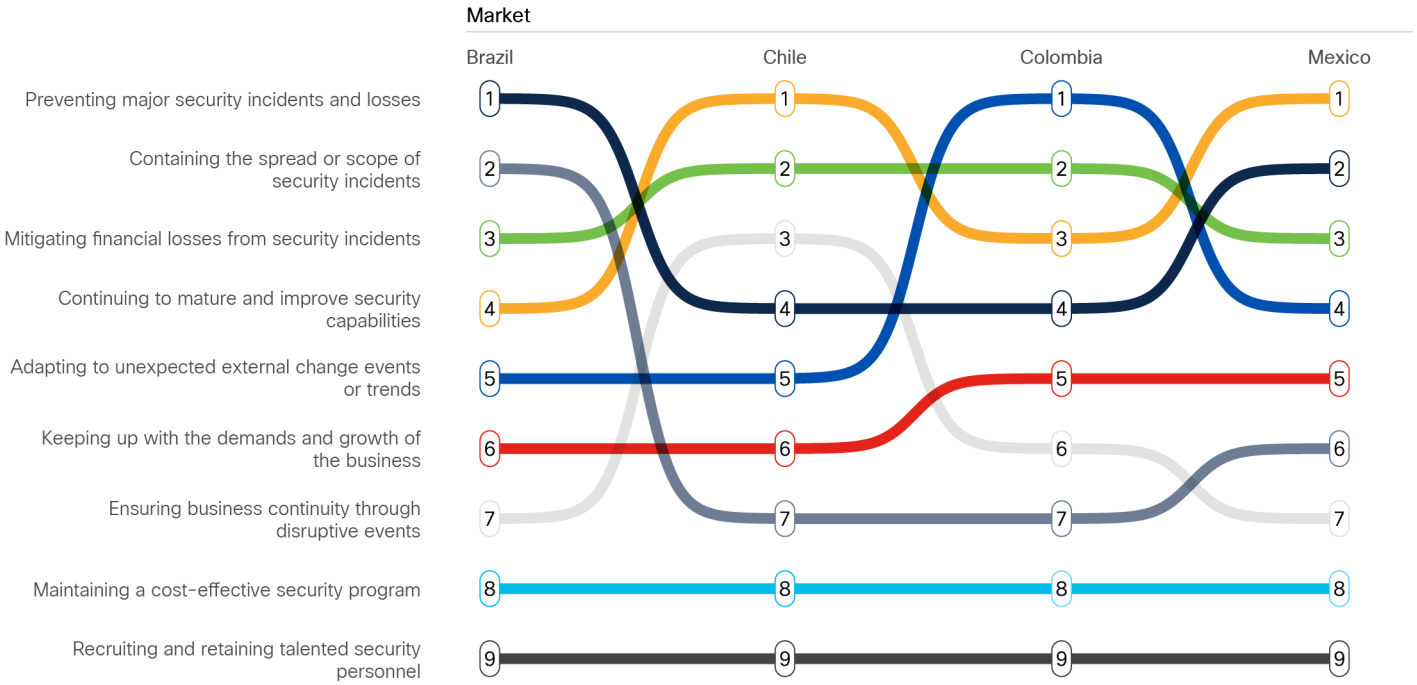
Source: Cisco Security Outcomes Report

Possible reasons behind the variation in incident rates, types, and impacts among markets include differences in regulatory and compliance pressures, geopolitical factors, prevalent business models, incident detection capabilities, and security program maturity to name but a few.

Which resilience outcomes are highest priority?

The main report presents nine core objectives or outcomes related to security resilience. We asked participants which of those nine outcomes their organizations considered to be the most important, and rankings for LATAM markets are shown below. Maintaining cost-effective programs and recruiting/retaining security talent rank as the lowest priorities across all markets. But there's quite a bit of variation among the other outcomes. For instance, containing the spread and scope of security incidents is the second highest priority outcome in Brazil but falls to #7 in Chile and Colombia.

Figure 4: Ranked importance of security resilience outcomes

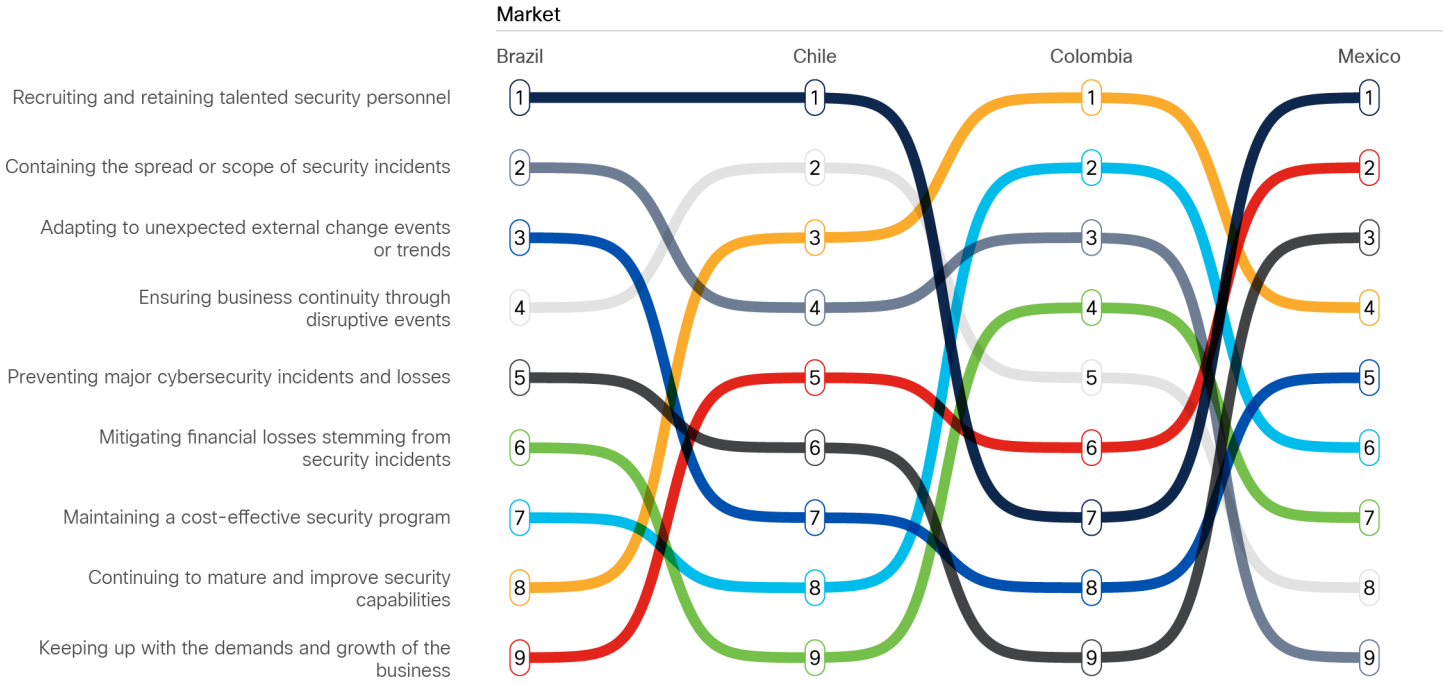


Source: Cisco Security Outcomes Report

Which resilience outcomes are hardest to achieve?

We also asked respondents to rate how well their organizations actually achieve each of the resilience outcomes. The chart below ranks the relative challenge associated with each outcome and traces how that ranking changes across LATAM. It's interesting to see how each market faces difference challenges. By way of example, continuing to mature and improve security capabilities is the biggest challenge for organizations in Colombia but purportedly much less challenging (#7) to those in Brazil. (It's worth the effort: Research shows a mature program more than doubles the effects of efforts to improve an organization's culture of security.) On the other hand, Colombian organizations seem to have little difficulty recruiting and retaining security personnel, while the other three LATAM markets consider that their biggest challenge.

Figure 5: Ranked difficulty of achieving security resilience outcomes

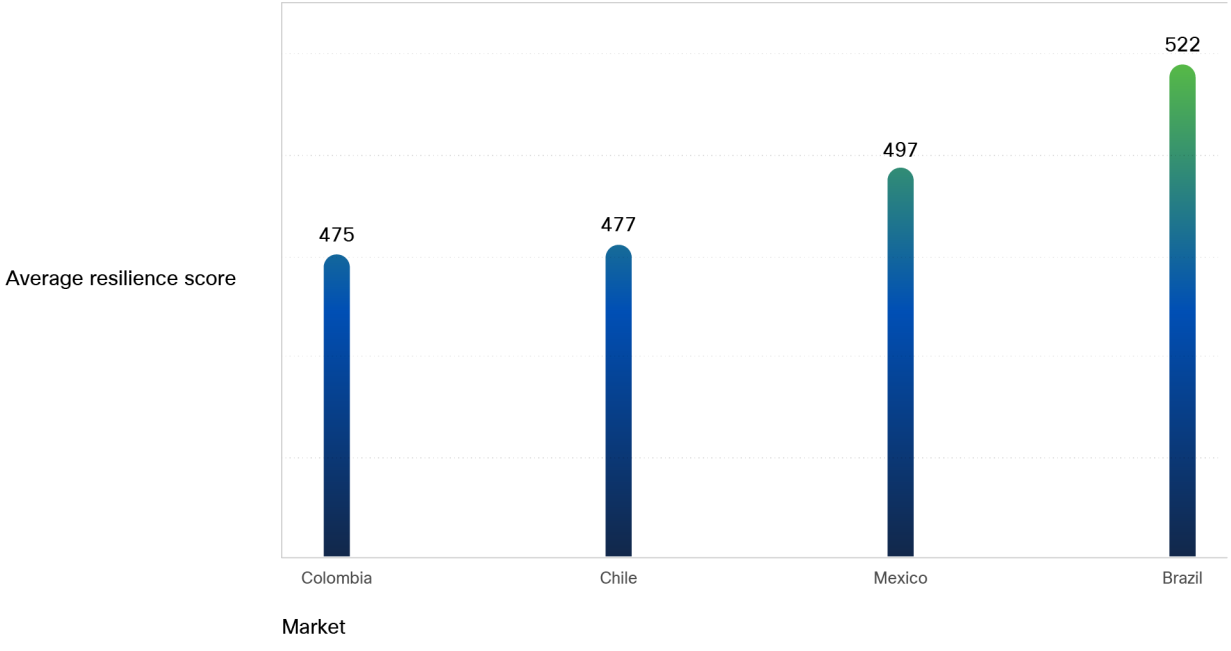


Source: Cisco Security Outcomes Report

Can we measure overall security resilience?

Based on ratings across the nine outcomes, we created an aggregate security resilience score for each organization. These scores were normalized such that the global average stands at 500. Overall, three of four LATAM markets underperformed that global average. Organizations in Colombia exhibit the lowest average security resilience score (475), while Brazil achieved the highest (522).

Figure 6: Average security resilience score for organizations in each market



Source: Cisco Security Outcomes Report

Improving security resilience

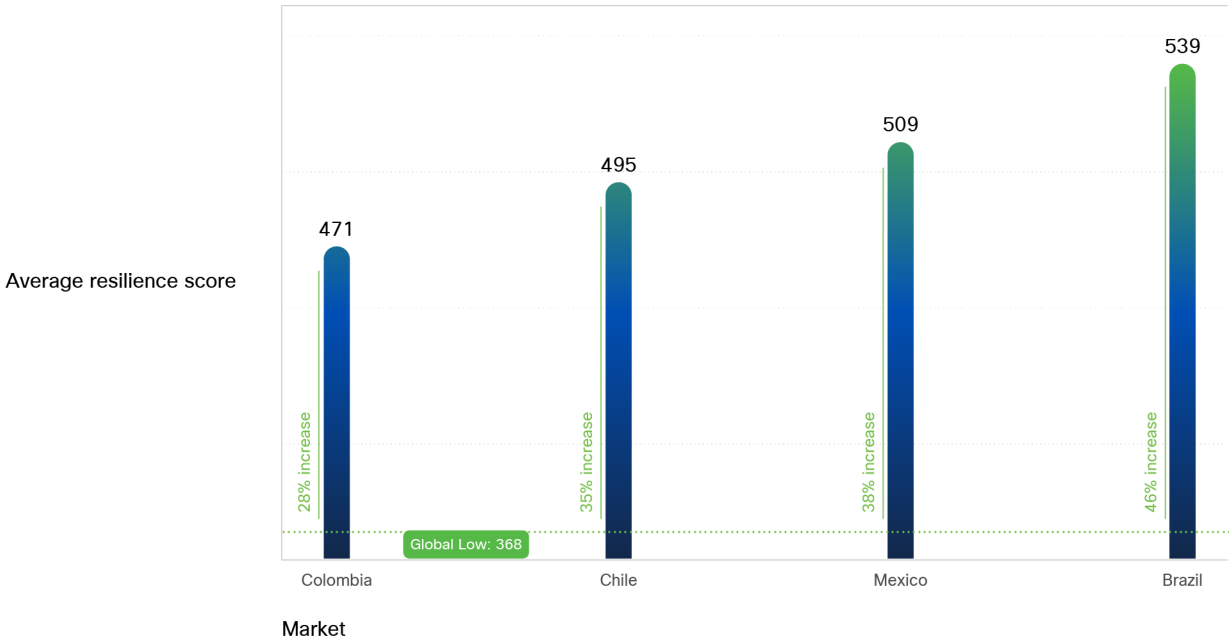
With a score representing overall security resilience across nine outcomes for each organization in the LATAM region, we tested numerous factors and identified seven that measurably improve those outcomes. We now show the range of potential improvement to overall security resilience scores associated with a few of these factors specific to LATAM.

Establish executive support

Globally, we observed that organizations reporting poor support from top executives exhibit security resilience scores that are 39% lower than those with strong C-suite backing. We offer a few clues from the data in the main report on how to garner such support. Here, we're interested in determining whether markets in LATAM exhibit similar effects.

The following chart presents the average security resilience score (blue bar) among organizations in each market with strong executive backing for their security program. The percentage increase on the side of those bars measures the total potential range of improvement over organizations lacking exec support. This enables us to observe that, for example, organizations in Colombia do benefit from strong executive support (+28% to average security resilience scores), but the increase is not as prominent as the global average of +39%. Those in Brazil, however, experience a larger boost of +46% when they're backed with strong executive support.

Figure 7: Potential effect of executive support on security resilience



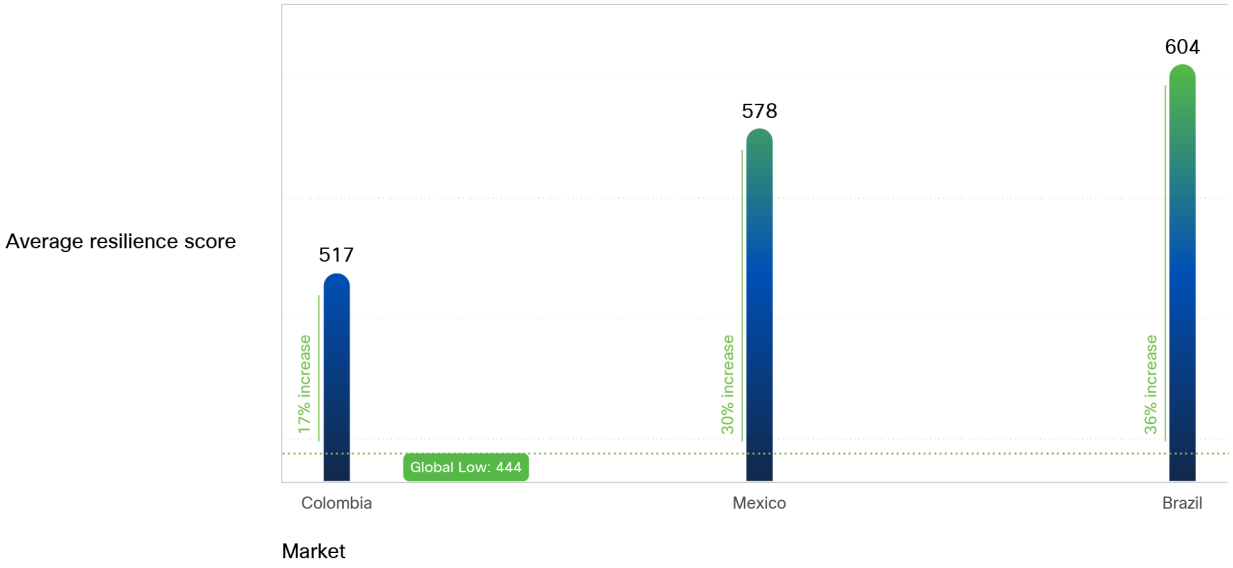
Source: Cisco Security Outcomes Report

Maximize zero trust adoption

The main report measured a 30% difference in average resilience scores between organizations that have made no progress toward implementing zero trust principles and those that have mature implementations (they have MFA, continuous validation, and micro-segmentation with adaptive policies, extensive monitoring, and orchestration of user workflows).

For the most part, LATAM markets show similar resilience improvements tied to zero trust.[1] Firms in Colombia see a relatively lower margin of increase (+17%) compared to the global average, while those in Brazil experience a twice that boost to security resilience (+36%) associated with mature zero trust implementations.

Figure 8: Potential effect of zero trust adoption on security resilience



Source: Cisco Security Outcomes Report

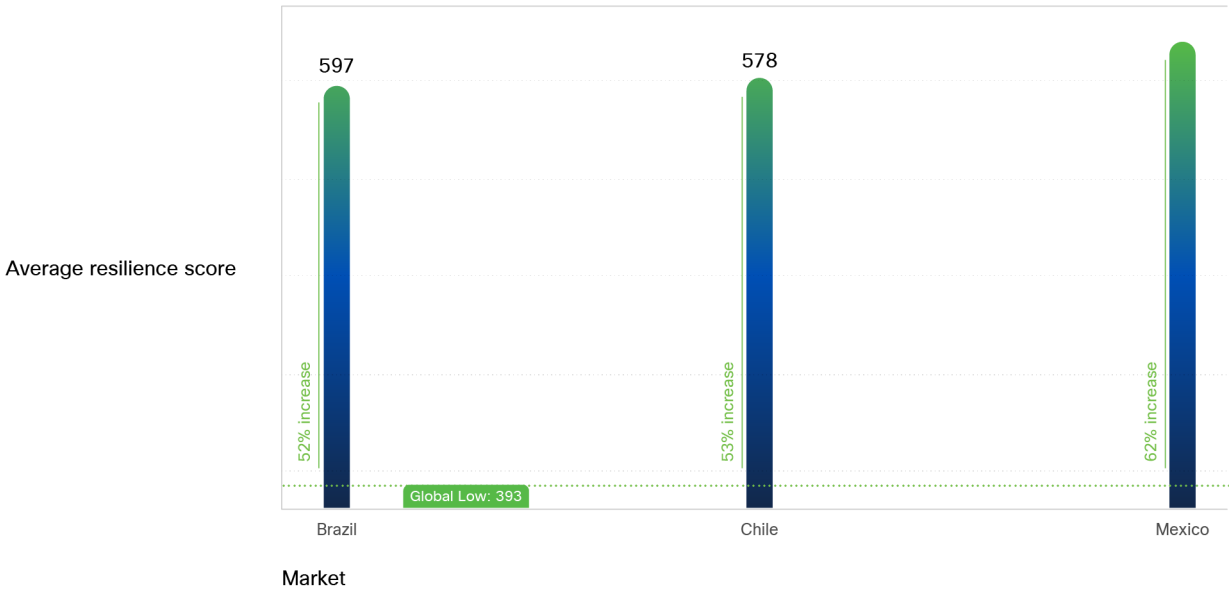
1 There were not enough participants in Chile reporting the lowest and highest levels of zero trust adoption to calculate the percentage increase to resilience score with a reasonable degree of confidence.

Extend detection and response capabilities

Modern cyber threats come at you from a multitude of vectors. It makes sense, then, that having multiple vantage points across those vectors would be an advantage for cyber defenses. Offering visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt for, and remediate threats is the core value proposition of extended detection and response (XDR) solutions.

Our data suggests that XDR delivers on that proposed value. Organizations with mature XDR implementations boasted overall resilience scores that were 45% higher than those without XDR capabilities. Per the figure below, average gains in key LATAM markets show even greater promise from XDR, rising from +52% in Brazil to +62% in Mexico.[2]

Figure 9: Potential effect of XDR adoption on security resilience



Source: Cisco Security Outcomes Report

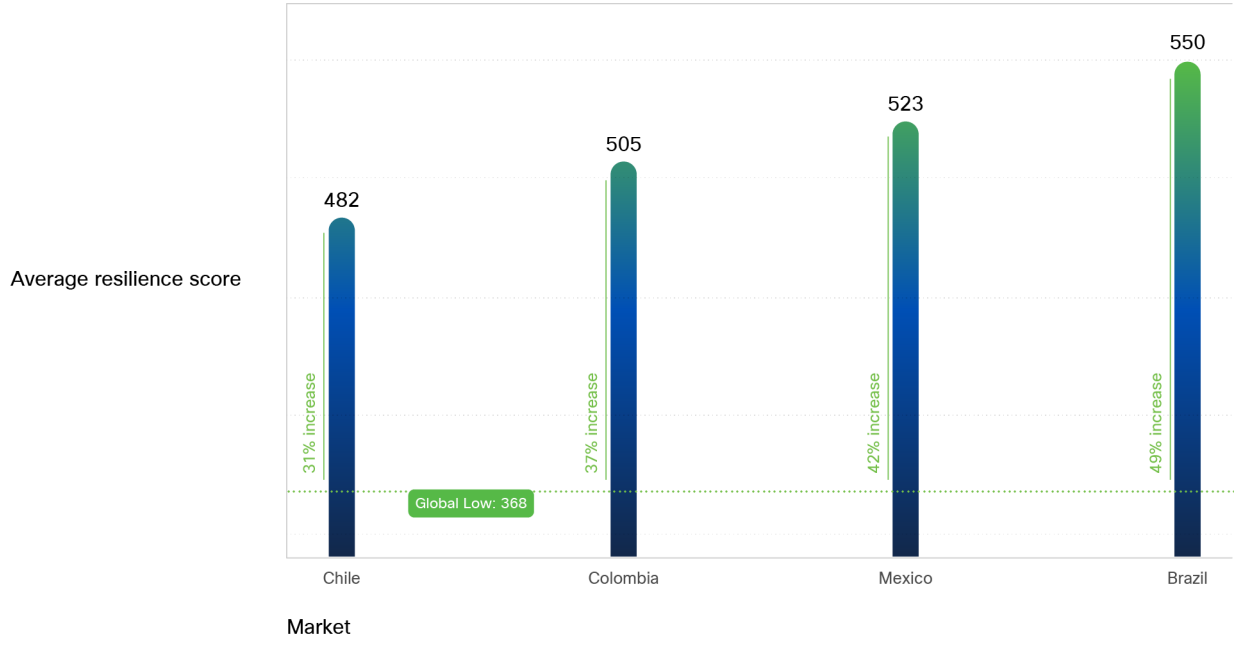
2 There were not enough participants in Colombia reporting the lowest and highest levels of XDR adoption to calculate the percentage increase to resilience score with a reasonable degree of confidence.

Take security to the edge

The acceleration in hybrid work – including a mobile workforce, the proliferation of devices, and the hyper-distribution of applications over multiple cloud providers – has resulted in growing challenges to securing this widespread, fragmented interconnectivity. Secure access service edge (SASE) offers a strategy to converge networking and security into a cloud-delivered service, simplify operations, and remain resilient in the face of ever-changing business demands. What's more, the latest Security Outcomes Report offers compelling evidence in support of SASE's efficacy.

Worldwide, we observed a 27% difference in average resilience scores between organizations with non-existent versus more mature SASE implementations (see what that includes here). Once again, all markets in LATAM show even larger gains of up to +49% (Brazil) over the baseline of firms that haven't started rolling out SASE.

Figure 10: Potential effect of SASE adoption on security resilience



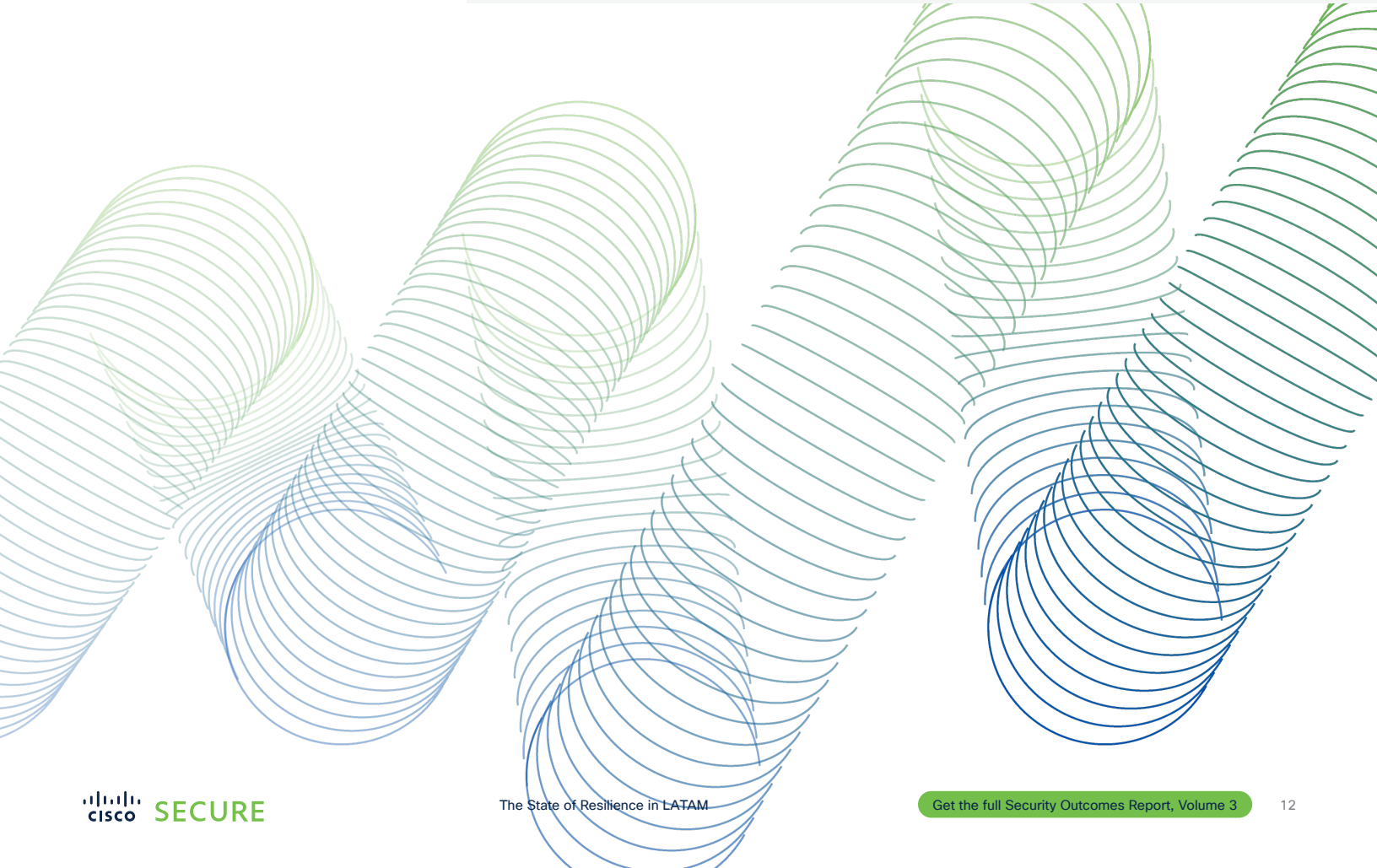
Source: Cisco Security Outcomes Report

Conclusion

While there is notable variation in responses across different countries and markets within the LATAM region, a few consistencies are worth exploring. Security resilience is a high priority for executives across the region, and organizations are aiming to develop their security capabilities. So, what can organizations do to address concerns around security resilience? The data clearly points to enhanced XDR capabilities, increased zero trust adoption, and mature SASE implementation as critical pathways to achieving greater resilience. Of course, optimizing each of these areas is a journey that requires planning and collaboration among IT and security operations teams.

Learn more:

To learn more about how teams can collaborate to reach their resilience goals, download the full Security Outcomes Report, Volume 3: Achieving Security Resilience.



CISCO
SECURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published March 2023

The bridge to possible