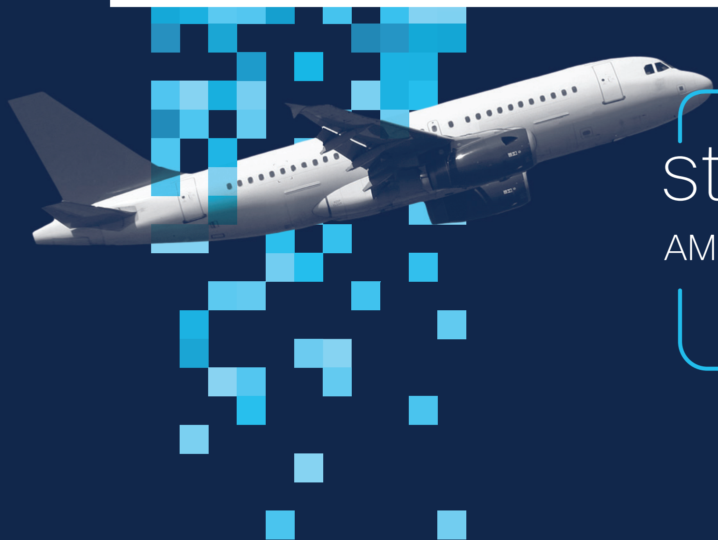
CISCO SECURE

SECURITY

OUTCOMES



study

AMER

Introduction

What makes a successful cybersecurity program? Is there evidence that security investments achieve measurable outcomes? How do we know what actually works and what doesn't? These are the types of burning questions guiding Cisco's 2021 Security Outcomes Study. This document is a companion to that study, focusing exclusively on findings specific to the Americas (Canada, United States, Mexico, and Brazil). Read on to discover how countries in the Americas region compare and what key factors contributed to the success of security programs like yours.

For the 2021 Security Outcomes Study, Cisco conducted a fully anonymous (source and respondent) survey of over 4,800 active IT, security, and privacy professionals from around the world. Of those participants, 1,059 represented firms headquartered in the Americas. An independent security research firm, the Cyentia Institute, provided analysis of the survey data and generated all results presented in this study.

Security Program Outcomes

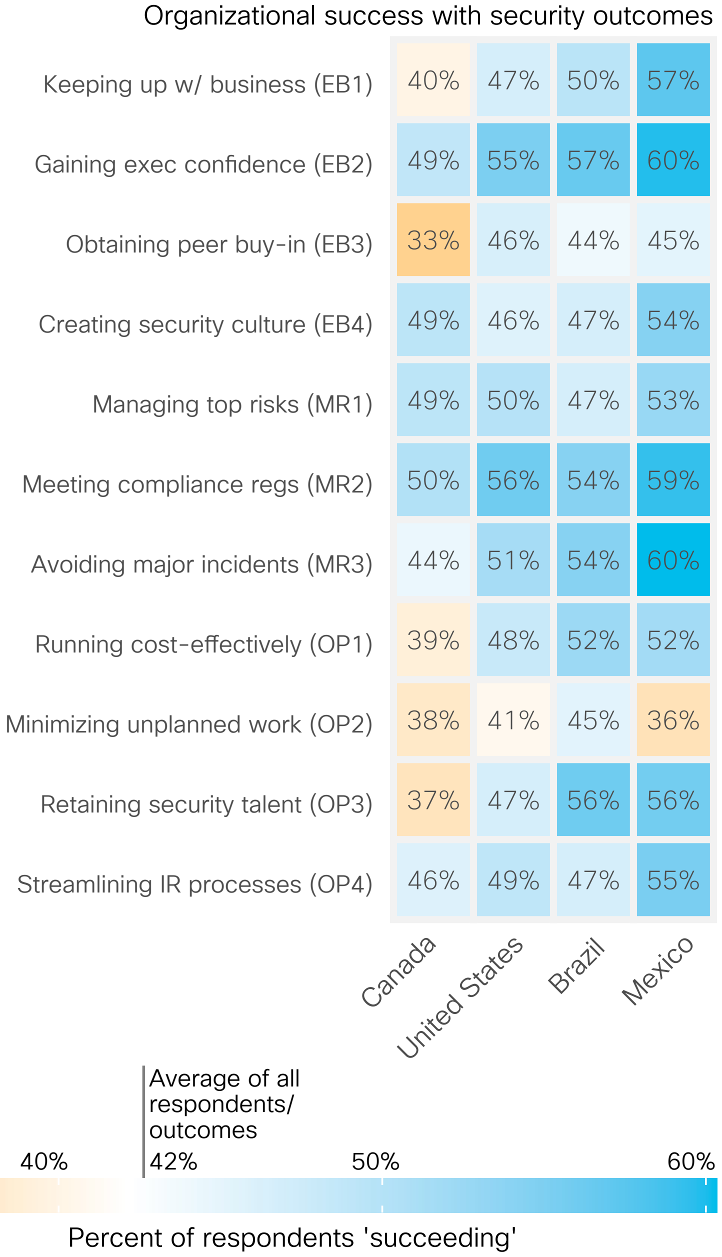
We asked respondents about their organization's level of success across 11 high-level security outcomes organized under three main objectives: Enabling the Business, Managing Risk, and Operating Efficiently.[1] Our ultimate goal was to identify security practices that drive successful outcomes, but let's not get ahead of ourselves. It's worth taking some time to see where various countries across the Americas region struggle and excel with these security outcomes relative to others.

[1] See Appendix B in the 2021 Security Outcomes Study for the full text for each outcome, along with the explanation and example evidence given to respondents to guide the rating of their programs' success.

Figure 1 shows the percentage of firms in each country that say their security program is successfully achieving each respective outcome in our list. So, for example, 40% of organizations in Canada say their security programs are keeping up with the business (upper-left square), 55% in Mexico are streamlining IR processes (lower-right square), and so on.

The coloring adds a dimension of relative performance to these values. Orange squares indicate that respondents generally report success rates below the global average; blue squares signify better-than-average outcomes. White squares indicate success rates roughly equal to the global average. From this, it's obvious that every country has different areas of struggle and success.

Figure 1: Country-level comparison of reported success rates for each security outcome



Organizational success with security outcomes

	Canada	United States	Brazil	Mexico
Keeping up w/ business (EB1)	40%	47%	50%	57%
Gaining exec confidence (EB2)	49%	55%	57%	60%
Obtaining peer buy-in (EB3)	33%	46%	44%	45%
Creating security culture (EB4)	49%	46%	47%	54%
Managing top risks (MR1)	49%	50%	47%	53%
Meeting compliance regs (MR2)	50%	56%	54%	59%
Avoiding major incidents (MR3)	44%	51%	54%	60%
Running cost-effectively (OP1)	39%	48%	52%	52%
Minimizing unplanned work (OP2)	38%	41%	45%	36%
Retaining security talent (OP3)	37%	47%	56%	56%
Streamlining IR processes (OP4)	46%	49%	47%	55%

Average of all respondents/ outcomes
40%
42%
50%
60%
Percent of respondents 'succeeding'

Source: Cisco 2021 Security Outcomes Study

We can't possibly compare and comment on every outcome for every country in Figure 1. But we can provide a few guidelines and share some general observations that should assist readers in drawing their own conclusions. Let's get to it.

Compare across columns for a country-centric reading of the chart. The countries are organized from left to right based on their relative performance across all outcomes. Based on that, we can easily see that respondents in Canada tend to **report** lower levels of success for every outcome, while those in Mexico generally **report** higher rates. The U.S. and Brazil fall right in the middle of that range. We've bolded "**report**" because it's important to the interpretation of these findings.

Figure 1 is a mix of actual and perceived success on the part of respondents, and it's impossible to know the ratio reflected in the percentages shown. Cultural factors are absolutely at play here, and we caution readers from making overly simplistic conclusions like "Security programs in Mexico are always more successful than in Canada." The opposite might in fact be true. Perhaps Canadian and U.S. firms set objectives based on stricter regulations, undergo regular audits of their security posture, and thus have a realistic understanding of where improvements need to be made. Perhaps the bar of what constitutes success varies across the region. Many other plausible explanations exist.

We know Figure 1 throws a lot of information at you. We suggest finding your country of interest along the bottom of the chart and then scanning up the column to see reported success rates for each outcome. The shading should help you quickly deduce where organizations in that country seem to be struggling (orange squares), succeeding (blue squares), and performing on par with the global average (white squares).

The point is to thoughtfully compare the country-level results in Figure 1. Consider what might be influencing responses in your country of interest and how that can help form a better understanding of what makes those programs tick. Furthermore, multinational organizations can use these results to rationalize diversity of perception and performance among security teams in different countries, so they can work better together as a unified program.

It's also possible to view Figure 1 from an outcome-centric perspective. This can be achieved by picking an outcome and comparing success rates across the row. Using this approach, it's apparent that all countries report reasonable success in meeting compliance regulations and gaining the confidence of executives (all blue squares). On the other hand, minimizing unplanned work seems to be more of a region-wide struggle (more orange squares). Again, perception plays into these findings, but such areas of consensus (or divergence) among respondents is quite interesting for understanding shared security challenges across a global community.

Overall, Figure 1 paints a diverse picture of security program success across the Americas region. But could that picture be improved even more for your organization and others in the region? Our data says yes. Head on to the next section to see what helped firms in each country boost their security program performance to the next level.

Looking for a broader, country-level view of program outcomes?

You're in luck! We've created an interactive data visualization that lets you further explore success rates for the countries shown in Figure 1, and for regions outside the Americas as well. Each country is benchmarked against the global average, enabling you to see exactly where local firms are struggling and succeeding to achieve security outcomes.

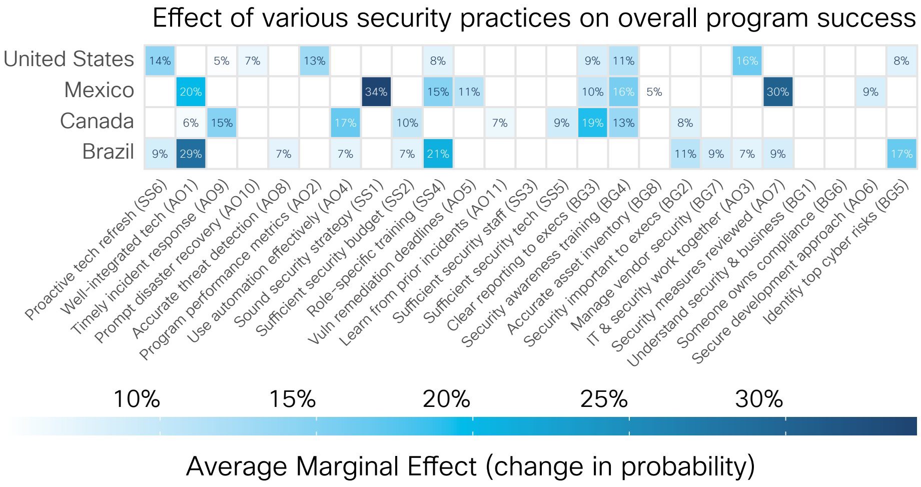
Key Success Factors

In addition to the outcomes above, we asked study participants how well their organizations followed a set of 25 common security practices.[2] We then conducted multivariate analysis to measure which of these practices correlate most strongly with achieving the outcomes above. In other words, what factors contribute to successful security programs among firms in the Americas region? Let's find out.

The values in Figure 2 denote the average increase in the probability of overall security program success when organizations strongly adhere to a given practice. So, for example, firms from the United States that claimed to have a proactive tech refresh strategy were 14% more likely (on average) to report highly successful security programs (upper-left square). Brazilian companies able to accurately identify their top cyber risks boosted their success by an average of 17% (lower-right square). These values have fairly wide variation around them, but they give a good sense of the marginal effects organizations are most likely to see/report. And they suggest there's a lot of opportunity to meaningfully improve security program outcomes.

Intersections in Figure 2 with no shading or value indicate that our analysis did not find a statistically significant correlation between the practice and overall security success for that country. However, it's still possible that those practices correlate with specific outcomes from Figure 1.

Figure 2: Contribution of security practices to rating of overall program success


Effect of various security practices on overall program success

	Proactive tech refresh (SS6)	Well-integrated tech (AO1)	Timely incident response (AO9)	Prompt disaster recovery (AO10)	Accurate threat detection (AO8)	Program performance metrics (AO2)	Use automation effectively (AO4)	Sound security strategy (SS1)	Sufficient security budget (SS2)	Role-specific training (SS4)	Vuln remediation deadlines (AO5)	Learn from prior incidents (AO11)	Sufficient security staff (SS3)	Sufficient security tech (SS5)	Clear reporting to execs (BG3)	Security awareness training (BG4)	Accurate asset inventory (BG8)	Security important to execs (BG2)	Manage vendor security (BG7)	IT & security work together (AO3)	Security measures reviewed (AO7)	Understand security & business (BG1)	Someone owns compliance (BG6)	Secure development approach (AO6)	Identify top cyber risks (BG5)
United States	14%		5%	7%		13%				8%					9%	11%				16%					8%
Mexico		20%						34%		15%	11%				10%	16%	5%				30%			9%	
Canada		6%	15%				17%		10%			7%		9%	19%	13%		8%							
Brazil	9%	29%			7%		7%		7%	21%								11%	9%	7%	9%				17%

Source: Cisco 2021 Security Outcomes Study

[2] See Appendix C in the 2021 Security Outcomes Study for the full text and listing of these practices.

Similar to Figure 1, Figure 2 can be read with a column- or row-centric view. And also like the previous section, we can't anticipate and comment on everything you might like to know about these results. But we absolutely want to equip you to gain as much insight as possible, so here are some tips to make the most of that effort.

Scanning across columns distinguishes practices that appear to provide a strong contribution to security success across much of the region (e.g., a well-integrated technology stack), as well as those with more localized effects (e.g., developing a sound security strategy in Mexico). The latter example brings up something to keep in mind while interpreting these results. The fact that three of four countries show no effect in the 'Sound security strategy' column doesn't mean programs in those countries don't need a good strategy. It just means we didn't observe significant additional benefit from improving security strategies beyond where they generally stand now. The data suggests that developing a sound strategy could be a current challenge facing many security programs in Mexico, and thus, it's a key differentiator for achieving more successful programs.

To get the most from Figure 2, locate your country of interest along the left side and then scan horizontally to find hot spots (blue squares). When you find one, follow the column down to identify the security practice behind that hot spot. The more intense the blue, the more that practice drives security success for organizations in that country. Thus, it's a quick way to get some data-backed recommendations to improve your security program.

Beyond individual countries, multinational companies can use this approach to identify practices that contribute to success across multiple areas in which they operate. This is a good opportunity to bolster weaknesses and build on strengths across international teams.

Following the rows in Figure 2 highlights practices that increase the chance of success for security programs in specific countries. For example, firms in the United States may benefit from removing barriers so that IT, development, and security teams can work together more effectively. Establishing a proactive technology refresh strategy to maintain a modern infrastructure appears to be a sound investment as well.

As mentioned earlier, organizations in Mexico might want to focus on developing their security strategy (+34% average success rate). Reviewing security measures to make sure they're supporting the execution of that strategy (+30%) looks to be a good bet too.

Establishing clear security reporting to executive leadership boosts the likelihood of success according to many Canadian security professionals we surveyed. At a more technical level, the effective use of automation across processes and technologies also holds promise.

Brazilian firms may wish to work on improving technology integration for a near 30% increase in program success. Leveling up security staff through role-based training and working to identify top cyber risks appear helpful for this region as well.

Overall, we find it both fascinating and encouraging that every country has multiple, evidence-backed options on the table for positively impacting the performance of security programs.

> “The bad guys are now moving at the speed of the machine, so our automation principle is to move at that same speed.Cisco solutions allow us to do so.”
>
> Jesse Beauman, M.S. Assistant Vice Chancellor for Enterprise Infrastructure, University of North Carolina at Charlotte

About Cisco Secure

At Cisco, we empower the security community with the reliability and confidence that they’re safe from threats now and in the future with the Cisco Secure portfolio and Cisco SecureX platform. We help 100 percent of Fortune 100 companies protect what’s now and what’s next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Get inspired by the latest security success stories shared by Cisco customers: https://www.cisco.com/go/secompanies.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

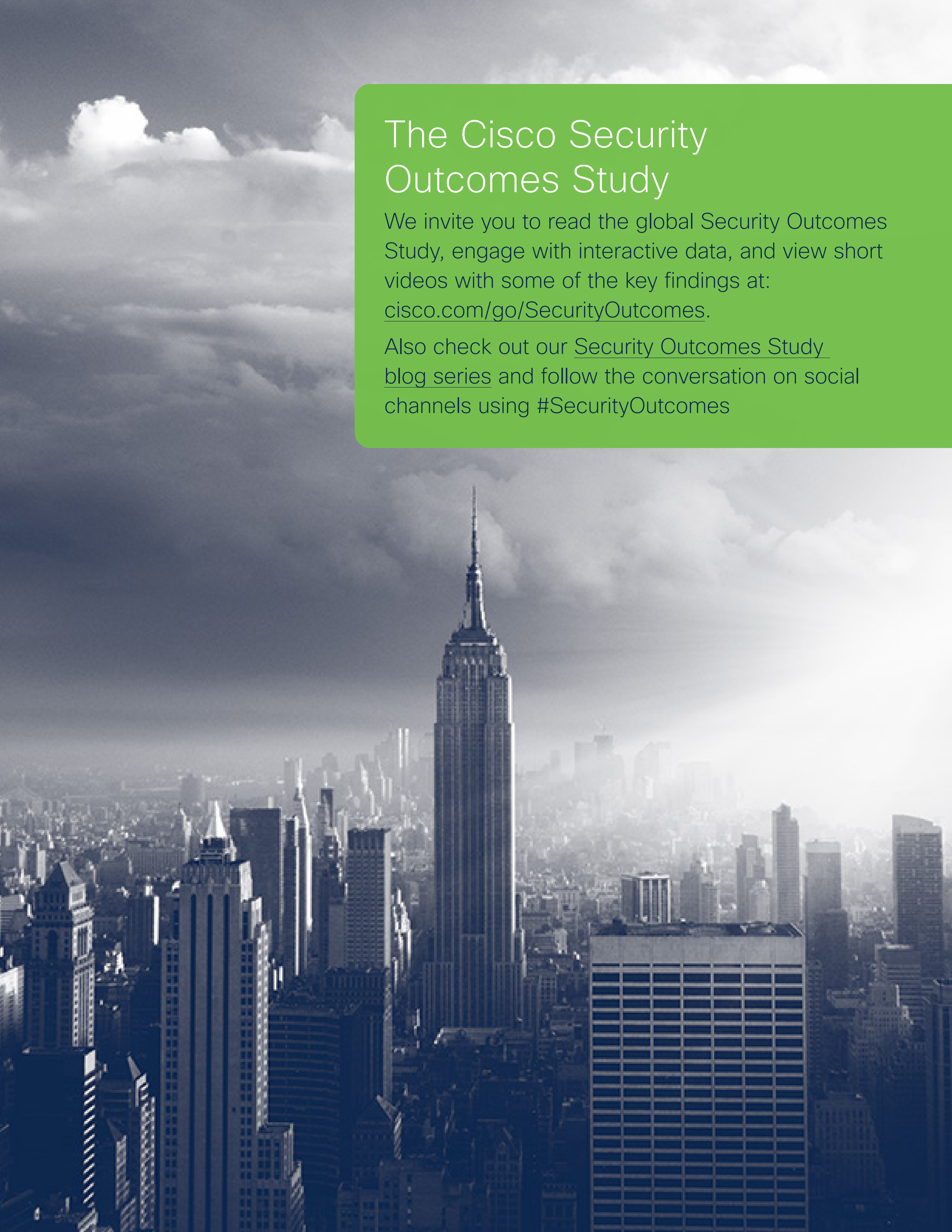
Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published December 2020

AMERRPT_12_2020

CISCO SECURE



The Cisco Security Outcomes Study

We invite you to read the global Security Outcomes Study, engage with interactive data, and view short videos with some of the key findings at: cisco.com/go/SecurityOutcomes.

Also check out our Security Outcomes Study blog series and follow the conversation on social channels using #SecurityOutcomes

CISCO
SECURE

CISCO The bridge to possible