CISCO SECURE

SECURITY

OUTCOMES

study

EMEAR

Introduction

What makes a successful cybersecurity programme? 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 Europe, Middle East, Africa, and Russia (EMEAR). Read on to discover how countries in the EMEAR region compare and what key factors contributed to the success of security programmes 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, 1,679 represented firms headquartered in EMEAR. An independent security research firm, the Cyentia Institute, provided analysis of the survey data and generated all results presented in this study.

Security Programme Outcomes

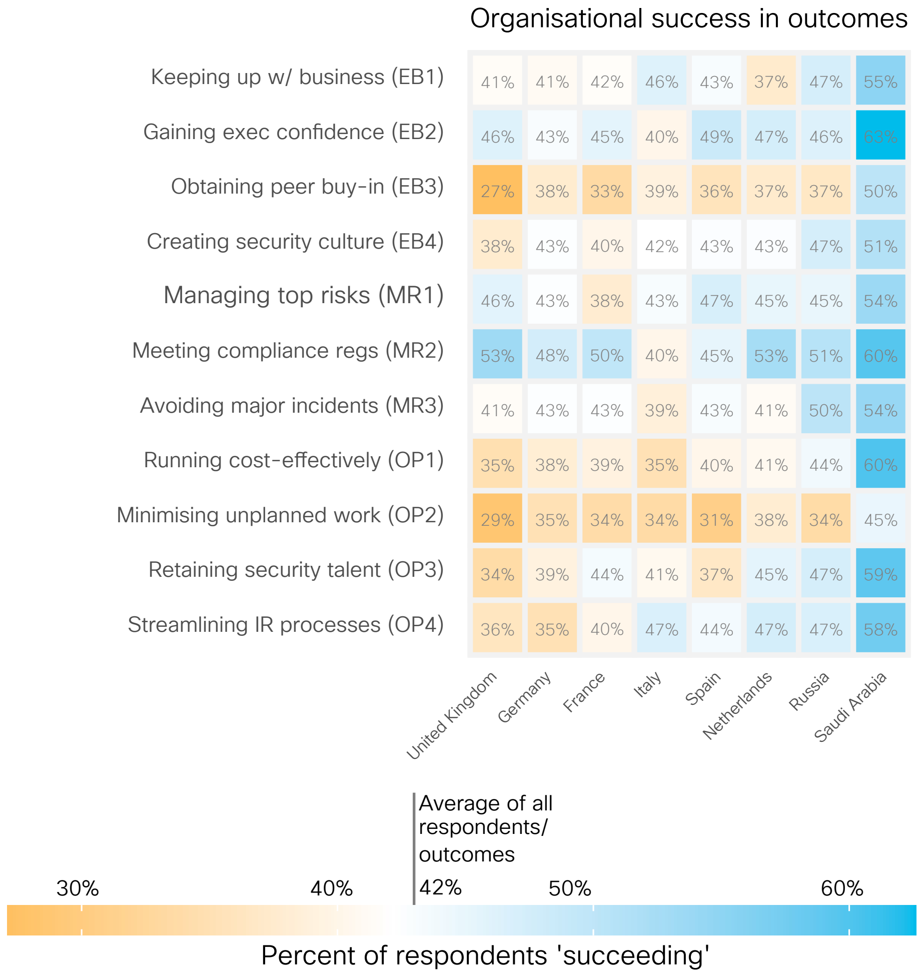
We asked respondents about their organisation's level of success across 11 high-level security outcomes organised under three main objectives: Enabling the Business, Managing Risk, and Operating Efficiently.[1] Our ultimate goal was to identify security practices that drive successful outcomes, but let's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

Figure 1 shows the percentage of firms in each country that say their security programme is successfully achieving each respective outcome in our list. So, for example, 41% of organisations in the UK say their security programmes are keeping up with the business (upper-left square), 58% in Saudi Arabia are streamlining incident response processes (lower-right square), and so on.

The colouring 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



Organisational success in outcomes

	United Kingdom	Germany	France	Italy	Spain	Netherlands	Russia	Saudi Arabia
Keeping up w/ business (EB1)	41%	41%	42%	46%	43%	37%	47%	55%
Gaining exec confidence (EB2)	46%	43%	45%	40%	49%	47%	46%	63%
Obtaining peer buy-in (EB3)	27%	38%	33%	39%	36%	37%	37%	50%
Creating security culture (EB4)	38%	43%	40%	42%	43%	43%	47%	51%
Managing top risks (MR1)	46%	43%	38%	43%	47%	45%	45%	54%
Meeting compliance regs (MR2)	53%	48%	50%	40%	45%	53%	51%	60%
Avoiding major incidents (MR3)	41%	43%	43%	39%	43%	41%	50%	54%
Running cost-effectively (OP1)	35%	38%	39%	35%	40%	41%	44%	60%
Minimising unplanned work (OP2)	29%	35%	34%	34%	31%	38%	34%	45%
Retaining security talent (OP3)	34%	39%	44%	41%	37%	45%	47%	59%
Streamlining IR processes (OP4)	36%	35%	40%	47%	44%	47%	47%	58%

Average of all respondents/ outcomes
30%
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 organised from left to right based on their relative performance across all outcomes. Based on that, we can easily see that respondents in the UK tend to **report** lower levels of success for many outcomes, while those in Saudi Arabia generally **report** higher rates.

We've bolded "**report**" in that last sentence because it's important to the interpretation of these findings. What we see in 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 "Saudi Arabian security programmes are always more successful than UK programmes." The opposite might in fact be true. Perhaps UK firms set objectives based on stricter regulations, undergo regular audits of their security posture, and have a keen sense of where risk exceeds tolerable levels. A healthy scepticism is better than unwarranted optimism when it comes to managing cyber risk.

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 organisations 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 programmes tick. Furthermore, multinational organisations can use these results to rationalise diversity of perception and performance among security teams in different countries, so they can work better together as a unified programme.

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 many countries report success in 'Meeting compliance regs' (more blue and white squares), while 'Minimising 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 programme success across the EMEAR region. But could that picture be improved even more for your organisation 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 programme performance to the next level.

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

You're in luck! We've created an interactive data visualisation that lets you further explore success rates for the EMEAR countries shown in Figure 1, and for other regions 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

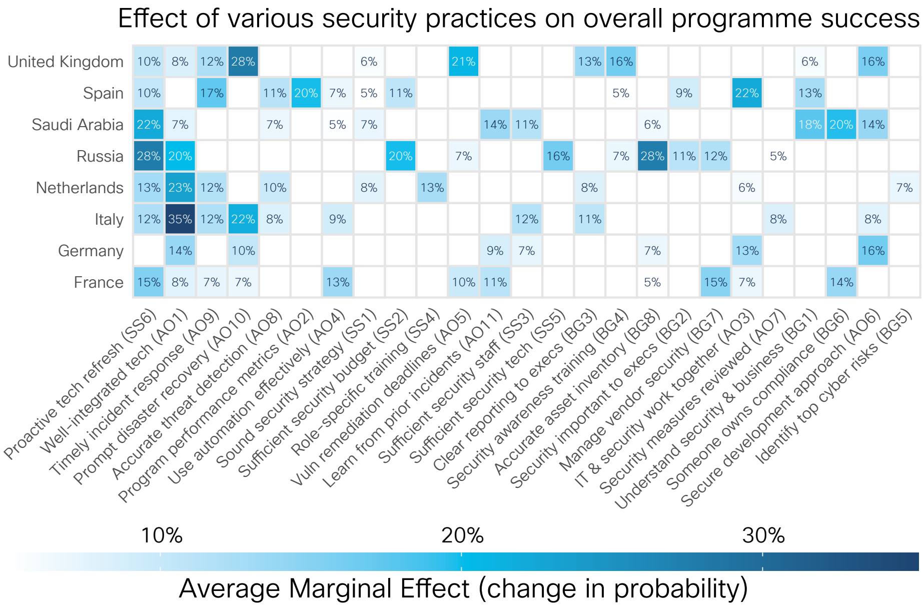
In addition to the outcomes above, we asked study participants how well their organisations followed a set of 25 common security practices.[2] We then conducted multivariate analysis to measure which of these practices correlate most strongly with achieving the outcomes above. In other words, what factors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

The values in Figure 2 denote the average increase in the probability of overall programme success when organisations strongly adhere to a given practice. So, for example, firms from France that claimed to have a proactive tech refresh strategy were 15% more likely (on average) to report highly successful security programmes (lower-left square). By comparison, organisations in Germany saw more net benefit from integrating their IT and security technologies than from refreshing them.

Intersections with no shading or value indicate that our analysis did not find a statistically significant correlation between the practice and overall success for that country. However, it's still possible that those practices correlate with specific outcomes from Figure 1, we might just need a bigger sample to detect the effect.

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.

Figure 2: Contribution of security practices to rating of overall programme 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 Kingdom	10%	8%	12%	28%				6%			21%				13%	16%						6%		16%	
Spain	10%		17%		11%	20%	7%	5%	11%							5%		9%		22%		13%			
Saudi Arabia	22%	7%			7%		5%	7%				14%	11%				6%					18%	20%	14%	
Russia	28%	20%							20%		7%			16%		7%	28%	11%	12%		5%				
Netherlands	13%	23%	12%		10%			8%		13%					8%					6%					7%
Italy	12%	35%	12%	22%	8%		9%						12%		11%						8%			8%	
Germany		14%		10%								9%	7%				7%			13%				16%	
France	15%	8%	7%	7%			13%				10%	11%					5%		15%	7%			14%		

Source: Cisco 2021 Security Outcomes Study

Scanning across columns distinguishes practices that appear to provide a strong contribution to success across the region (e.g., a proactive tech refresh strategy) as well as those with more localised effects (e.g., reviewing security measures in Russia or identifying top cyber risks in the Netherlands). Multinational companies can use this approach to identify practices that contribute to success across multiple countries in which they operate.

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

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 organisations in that country. Thus, it's a quick way to get some data-backed recommendations to improve your security programme.

Following the rows in Figure 2 highlights practices that increase the chance of success for security programmes in specific countries. For example, organisations in Italy might want to focus on integrating their technology stack (+35% average success rate). Firms in the UK may receive a high ROI from investing in disaster recovery measures (+28% average success rate). The list goes on. We find it both fascinating and encouraging that every country has multiple, evidence-backed options available to positively impact the performance of security programmes.

> "I'm thrilled with the many improvements we've made by choosing Cisco for our SASE architecture. We have supercharged the supermarket experience and have become one of the most beloved brands in the Kingdom."
>
> Joel Marquez, IT Director at Tamimi Markets, Saudi Arabia

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 January 2021

EMEARRPT_01_2021

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