cisco SECURE

Cisco Cybersecurity Readiness Index

From a static to a dynamic world

February 2023

Executive Summary

What was once deemed as the “future of work” has turned into a reality over the past couple of years. Of the many changes brought about by the COVID-19 pandemic, the most profound has been how business has shifted to enable hybrid work as the norm.

Companies across the globe have seen first-hand the positive aspects of hybrid work. Today, organizations are figuring out how to optimize the ability to bring people together physically, while giving employees the flexibility to which they have become accustomed.

Organizations need to protect three key aspects of business – workforce, workplace, and workloads. They are now having to do so in a rapidly evolving environment which presents a new challenge to IT teams. What was once a static environment – with people and devices in a specific location accessing static applications – has become an ever-moving, hybrid environment where people, devices, applications, and data can be in multiple, changing locations.

In the context of this environment, we wanted to gauge the cybersecurity readiness of organizations globally. To measure this, we looked at five key aspects from a security perspective - **identity**, **devices**, **network**, **application workloads**, and **data** - areas critical to organizations in their current operating environment.

We conducted a double-blind survey of 6,700 cybersecurity leaders from across the globe to understand whether their companies had solutions in place to meet the challenges of each pillar, and how far along they were towards full deployment of these solutions. All in all, we asked respondents to share the deployment of 19 different capabilities under the five areas to assess their readiness.

Each capability was assigned an individual weighting based on its relative importance to helping safeguard that aspect. The scores for each organization were then derived based on the stage of deployment of various solutions under each of the five pillars, with partially deployed solutions assigned 50% weighting and fully deployed solutions weighted at 100%.

Based on the overall score, the companies are placed in four stages of readiness for each pillar:

- **Beginner (Less than 10):** Organizations at the start of the cybersecurity readiness journey.
- **Formative (11 – 44):** Performing below average on cybersecurity readiness.
- **Progressive (45 – 75):** Performing above average on cybersecurity readiness.
- **Mature (76 and higher):** High performing with a mature and robust cybersecurity strategy.

This paper presents the initial findings of the survey.

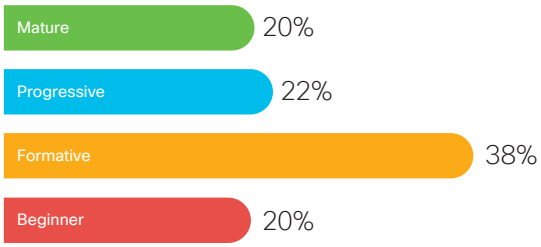
Identity

Our research underlines the challenge on this front: a quarter (24%) of all respondents ranked Identity Management as the number one risk for cyberattacks. Because of this, it is no surprise that 95% of our respondents have implemented some kind of identity management solution, with Integrated Identity and Access Management proving most popular, with two-thirds saying they have deployed these solutions.

There is significant progress to be made to meet the challenge of identity verification. Only one in five organizations (20%) fall into the Mature category, with a similar number (22%) in the Progressive segment. Close to two in three organizations fall into the Formative (38%) or Beginner (20%) category, which is worrying given the clear threat presented by identity management.

Organizations perceive the biggest risk in these areas

Readiness to protect identity

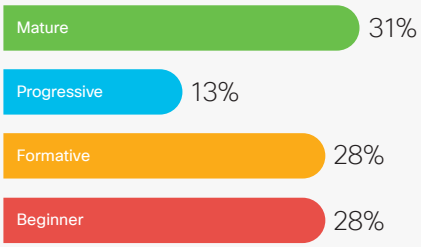


Devices

The number of devices that connect to a company network has grown exponentially in recent years. From laptops, phones and tablets, to devices such as security cameras, and smart printers, the list is almost endless. No matter what the device, if it is connected to the network, it needs to be protected.

The level of readiness to tackle the cybersecurity risks on this front varies. There is good news in that 31% of companies globally are in the Mature category, the highest of any pillar, with a further 13% at the Progressive stage. However, more than half (56%) of companies are either at the very start of their journey, or only a short way down the path.

Readiness to protect devices

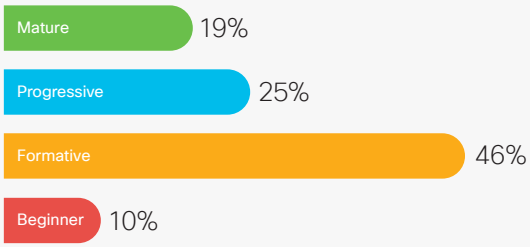


Network

A hybrid working environment calls for flexibility not only in the number and type of devices that employees use but also in where they log-in from, and where the data they need to access is stored and processed. That makes the role of the network even more important, and the need to safeguard it even more critical.

While our respondents recognize this, their organizations are lagging behind on their preparations to tackle the cybersecurity risks on this front. More than half of companies globally (56%) are either in the Formative or Beginner categories and just 19% sit in the Mature category - the most advanced state of readiness.

Readiness to protect networks

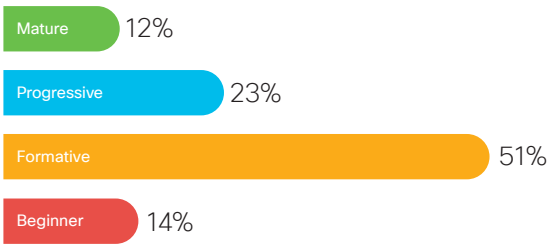


Application Workloads

The widespread adoption of applications across businesses, and their importance to customer experience, has added another layer of complexity for cybersecurity teams as malicious actors look at applications as yet another way they can try to infiltrate a company's IT infrastructure.

While companies globally have adopted tools and capabilities to safeguard themselves, the scale of deployment clearly has not kept pace with the speed at which applications have grown. Our survey shows that 65% of companies globally are in the Formative or Beginner stage, and only about 12% are in the Mature stage, the smallest number across the five areas that we have assessed.

Readiness to protect application workloads

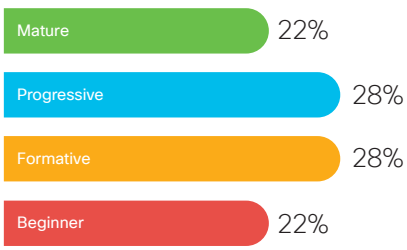


Data

Often labelled as the “new currency”, it is critical for companies to safeguard all forms of data in their ecosystem. Beyond it being the “right thing to do”, in most countries there are also regulatory requirements. Failure on this front can have serious implications for business, and our respondents recognize this.

The critical nature of data protection explains why the Mature and Progressive categories account for half (50%) of the respondents in our survey, a significantly higher proportion than we saw for device protection readiness, for example. However, there is work to be done as 22% companies are still in the Beginner stage – the second highest number in this stage across the five key areas.

Readiness to protect data



What do companies need to do to be prepared?

Building Security Resilience

Because threats are everywhere, we need to think about security differently. Stand-alone security strategies do not work anymore; they focus too much on threat prevention, end up siloed and treat all threats equally. What organizations need is security resilience, where the focus is on what matters most and anticipating what is coming down the road so the organization can bounce back faster when a threat becomes real. Most organizations are already thinking about resilience in how their financial, operations, organizational, and supply chains functions. Security resilience cuts across all of them. No company should claim it can protect you from all threats at all times. Resilience is about verifying threats, understanding connections across your organization, and seeing the full context of any situation so you can prioritize and ensure your next action is the best one.

There are five dimensions to security resilience:

1. **Close the gaps in your system so you have one, open platform**
2. **See more and always be monitoring**
3. **Anticipate what is next using actionable intelligence**
4. **Prioritize what matters most**
5. **Automate your response so you can bounce back fast**

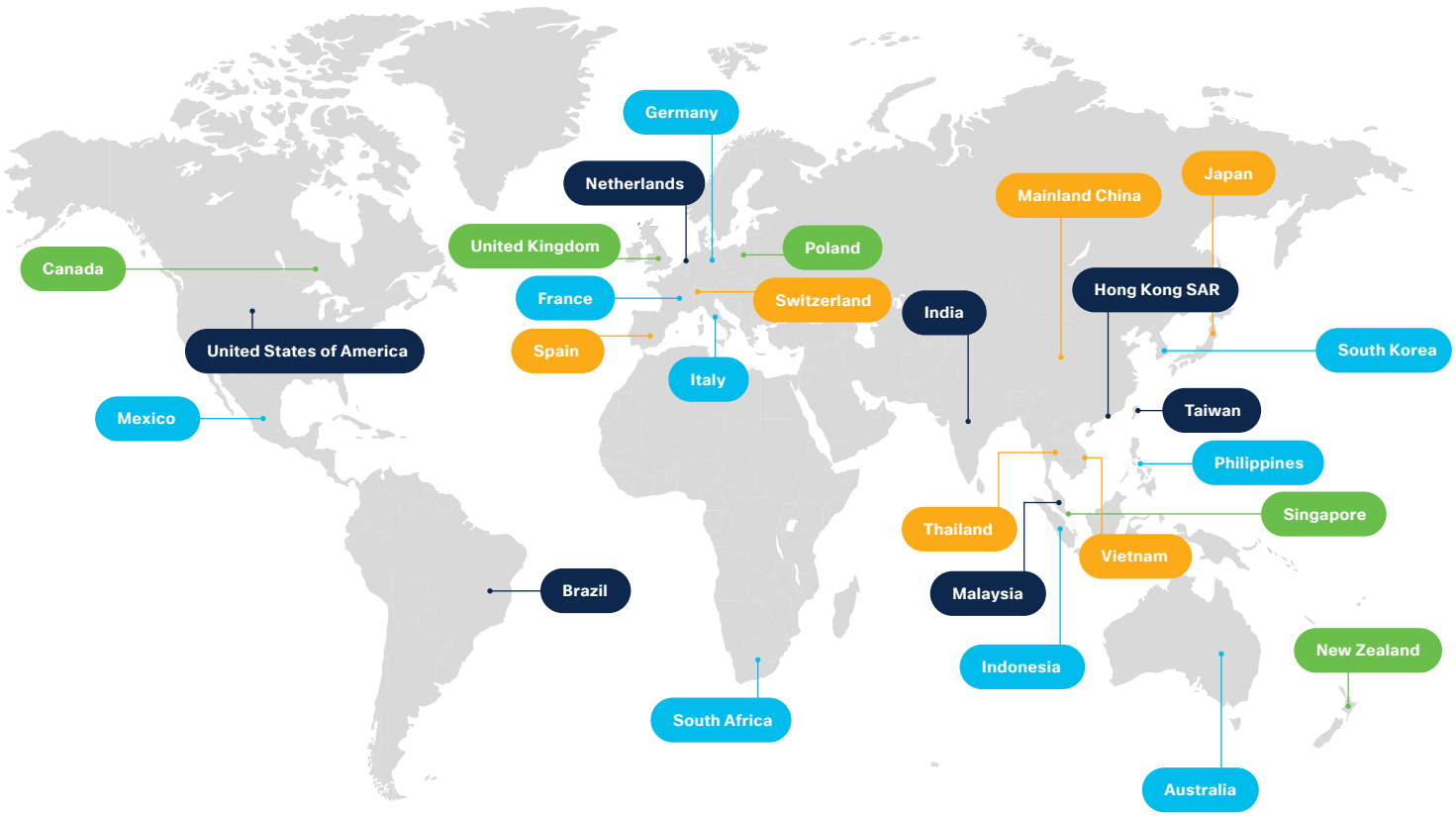
About the Survey

The Cybersecurity Readiness Index is based on data from a double-blind survey of 6,700 business leaders globally who have cybersecurity responsibilities in their organizations.

The organizations cover 27 markets in North America, Latin America, EMEA and Asia Pacific: Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Phillippines, Poland, Singapore, South Africa, South Korea, Spain, Switzerland, Taiwan, Thailand, UK, USA and Vietnam.

In relation to the five core pillars of cybersecurity protection: identity, devices, network, application workloads, and data, we looked at 19 different solutions across these pillars. Respondents were asked to indicate which of these they had deployed, the stage of deployment, and if these solutions were not already deployed then what budgets had been approved, and the intended timeline of deployment.

The research was carried out between August and September 2022 using online and telephone interviews.



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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**

The bridge to possible