cisco SECURE

Cisco Cybersecurity Readiness Index

Resilience in a Hybrid World

March 2023 | USA edition

Executive Summary

In a post COVID world, the requirements of cybersecurity have changed as the landscape for businesses has been spun on its head. Organizations have moved from an operating model that was largely static – where people operated from single devices from one location, connecting to a static network – to a hybrid world in which we increasingly operate from multiple devices in multiple locations, connecting to multiple networks.

While there is broad consensus that the move to hybrid is here to stay, its long-term success hinges greatly on organizations' ability to safeguard themselves against new and rapidly evolving threats.

Set against this, we wanted to understand how ready organizations around the world are to meet these modern security challenges. To do this, we developed the *Cisco Cybersecurity Readiness Index*. It categorizes companies into four stages of readiness: from **Beginner**, to **Formative**, **Progressive**, and finally **Mature**, based on their preparedness across five key pillars and the state of deployment of 19 security solutions within those.

The Global Cybersecurity Readiness Gap

The results are stark: according to the index, a mere 15% of organizations globally are deemed to have a mature level of preparedness to handle the security risks of our hybrid world. In the USA, the level of preparedness is even lower with only 13% of organizations falling into the Mature stage of readiness.

Most companies are aware that the threat is real, as 75% of security leaders that we spoke to in the USA believe cybersecurity incidents are likely to disrupt their businesses over the next 12 to 24 months. This compares to a global number of 82% who feel the same.

And the consequences of not being prepared have never been greater. 54% of respondents in the USA said they had

The five pillars of security protection


Identity


Devices


Network


Application Workloads


Data

experienced some kind of cybersecurity incident in the last 12 months, compared to 57% globally. The incidents cost 35% of American organizations affected at least US$500,000 or more, compared to 41% globally who had similar costs.

We have an alarming cybersecurity readiness gap, and it's only going to widen if global business and security leaders don't pivot quickly.

Closing the Cybersecurity Readiness Gap – Our Global Security Resilience Imperative

The good news is that security leaders are aware of the risks and are keen to invest in their cybersecurity readiness: 82% of American organizations have plans to increase their cybersecurity budget by at least 10% over the next 12 months, compared to 86% globally. It is crucial that these budget increases are delivered sooner rather than later. Given the environment that businesses operate in and the current readiness gap, a 12-month wait is far too long.

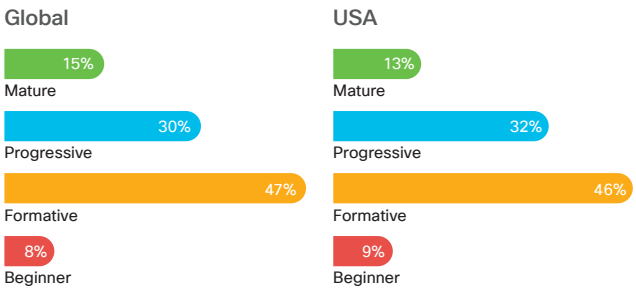
But as they deploy budgets, companies do need to think about security differently. Because threats are everywhere, stand-alone security strategies are no longer effective; they focus too much on threat prevention, create siloes that can be exploited, and don't account for the full business impact.

What organizations need is security resilience, where security is foundational to business strategy and is collectively prioritized throughout the organization, allowing companies to better anticipate threats and bounce back faster when a threat becomes real. Most organizations are already thinking about resilience in their financial, operational, organizational, and supply chain functions. Security resilience cuts across all of them. Resilience is about verifying threats, understanding connections across the organization, and seeing the full context of any situation so teams can prioritize and ensure their next action is the best one.

For business leaders to build secure and resilient organizations, they must establish a baseline of how 'ready' they are across the five major security pillars. The maturity of security infrastructure, particularly in relation to local and global peers, will help organizations identify what areas they are strong in and where they can best prioritize resources to improve their ability to be resilient. Our hope is that this Cybersecurity Readiness Index will act as a wake-up call for senior business leaders.

Closing this cybersecurity readiness gap must become a global imperative. We cannot afford to fall further behind as the shift to hybrid continues to accelerate. The impact on businesses, customers and society will only increase amid an explosion of hybrid threat vectors and an increasingly complex threat landscape. While some progress has been made, not enough firms are cybersecurity-ready to take on the challenges that our hybrid world has created.

Overall cybersecurity readiness of organizations



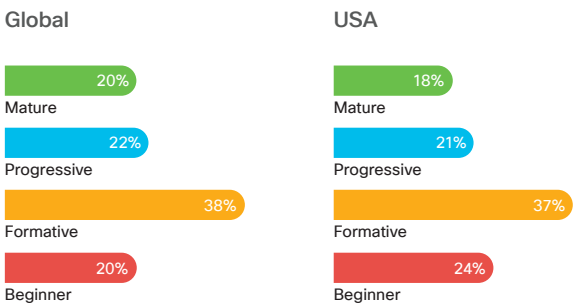
Identity

Our research underlines the challenge on the identity 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.

In the USA, 18% of organizations are at the Mature stage of readiness, 21% are at the Progressive stage, 37% are Formative, and 24% are Beginners.

Readiness to protect identity



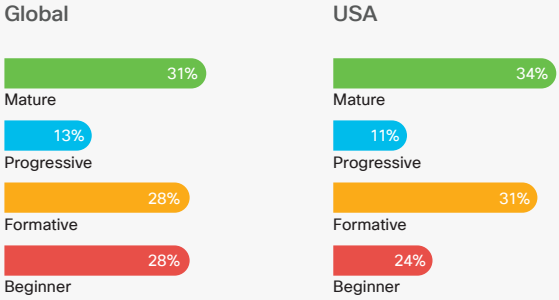
Devices

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.

In the USA, 34% of organizations are at the Mature stage of readiness, 11% are at the Progressive stage, 31% are Formative, and 24% are Beginners.

Readiness to protect devices



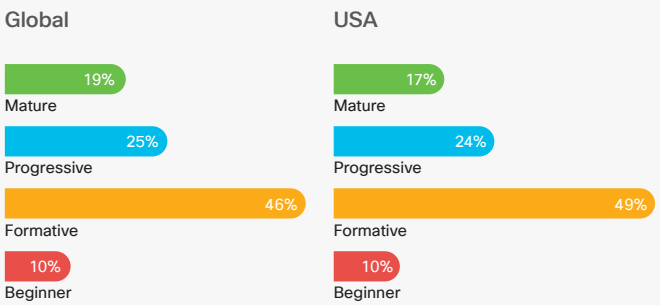
Network

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.

In the USA, 17% of organizations are at the Mature stage of readiness, 24% are at the Progressive stage, 49% are Formative, and 10% are Beginners.

Readiness to protect networks



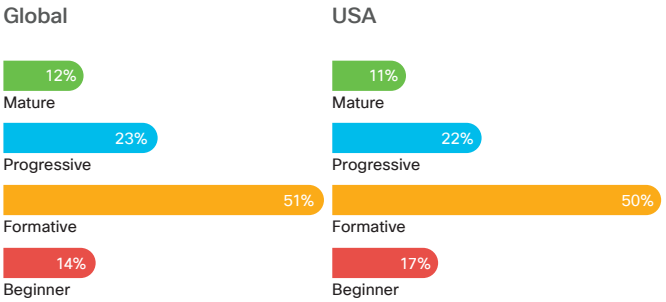
Application Workloads

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.

In the USA, 11% of organizations are at the Mature stage of readiness, 22% are at the Progressive stage, 50% are Formative, and 17% are Beginners.

Readiness to protect application workloads



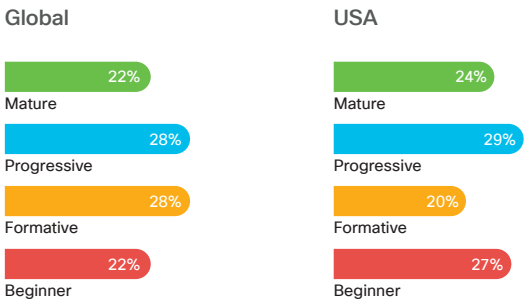
Data

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.

In the USA, 24% of organizations are at the Mature stage of readiness, 29% are at the Progressive stage, 20% are Formative, and 27% are Beginners.

Readiness to protect data



What do companies need to do to be prepared?

Building Security Resilience

In critical areas, significant steps have been taken to secure organizations against cybersecurity threats. However, organizations around the world – and perhaps governments – need to recognize that there is a long way to go. Deployments of some solutions, particularly those for identity, devices and networks, are not being rolled out as quickly as they could, leaving some organizations vulnerable to attack.

When the consequences of cyberattacks are so clear to see, resilience must be a priority for all organizations and deployment of solutions needs to be accelerated.

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 Research

The *Cybersecurity Readiness Index* is sourced from a double-blind survey of 6,700 private sector cybersecurity leaders. The organizations cover 27 territories in North America, Latin America, EMEA and Asia-Pacific: **Australia**, **Brazil**, **Canada**, **China**, **France**, **Germany**, **Hong Kong SAR**, **India**, **Indonesia**, **Italy**, **Japan**, **Malaysia**, **Mexico**, **Netherlands**, **New Zealand**, **Philippines**, **Poland**, **Singapore**, **South Africa**, **South Korea**, **Spain**, **Switzerland**, **Taiwan**, **Thailand**, **UK**, **USA** and **Vietnam**.

The index is based on five pillars: **Identity**, **Devices**, **Network**, **Application Workloads**, and **Data**. From within those pillars, we examined 19 different solutions required to address them. 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.

Each solution was assigned an individual weightage based on its relative importance to helping safeguard the applicable pillar. 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 a 50% weighting and fully deployed solutions weighted at 100%.

The scores for each pillar were then combined and weighted to arrive at an overall cybersecurity readiness score for each organization. The importance of each pillar was weighted as network (25%); identity (20%); devices (20%); data (20%); and application workloads (15%).

The respondents are drawn from 18 industries: business services; construction; education; engingeering, design, architecture; financial services; healthcare; manufacturing; media & communications; natural resources; personal care & services; real estate; restaurant services;retail; technology services; transportation; travel services; wholesale and 'others'.

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

Measuring Security Readiness – weightages

Identity

Capability	Weightage
Traditional data stores like AD	**30%**
Integrated IAM solution	**60%**
Privileged Access Management	**10%**

Pillar weightage: 20%

Devices

Capability	Weightage
Built-in protections in the OS such as AV and host controls	**10%**
Anti-virus with some enhanced features	**20%**
End-point protection platform (Firewall, malware, USB controls, process viability)	**70%**

Pillar weightage: 20%

Network

Capability	Weightage
Network segmentation policies based on identity	**40%**
Firewalls with built-in IPS	**25%**
Network behavior anomaly detections tools	**25%**
Packet capture and sensor tools	**10%**

Pillar weightage: 25%

Application Workloads

Capability	Weightage
Host software firewall	**15%**
Endpoint protection capabilities	**35%**
DLP	**10%**
Application centric protection tools	**20%**
Visibility and forensic tools	**20%**

Pillar weightage: 15%

Data

Capability	Weightage
Encryption tools	**10%**
Identification and classification with DLP	**20%**
Backup and recovery	**50%**
Host IPS & protection tools	**20%**

Pillar weightage: 20%

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