cisco SECURE

Cisco Cybersecurity Readiness Index

Resilience in a Hybrid World

March 2023

Contents

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.

A mere **15% of organizations globally are deemed to have a mature level of preparedness** to handle the security risks of our hybrid world.

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. More details on the scoring methodology can be found in the following section.

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.

This is despite most companies being aware that the threat is real. Four out of five (82%) security leaders we spoke to globally believe cybersecurity incidents are likely to disrupt their businesses over the next 12 to 24 months.

And the consequences of not being prepared have never been greater. Almost 60% of respondents said they had experienced some kind of cybersecurity incident in the last 12 months. The incidents cost 71% of organizations affected at least US$100,000, with 41% saying the overall cost was US$500,000 or more.

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

Almost **60% of respondents** said they had experienced some kind of **cybersecurity incident in the last 12 months**.

Mapping Readiness Around the World

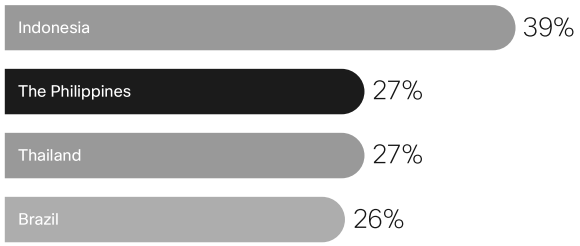
As you might expect, there are variations in private company cybersecurity readiness across markets, but not in the way we might ordinarily expect. In our index, private sector companies in less developed nations outperform their peers in wealthier countries by a considerable margin, especially in Asia-Pacific and the Americas.

In the Americas, **Brazil** stands out as the country where companies are most ready to tackle today's security challenges, with 26% of companies considered in a mature stage of preparedness. Meanwhile, companies in **Canada** (9% in Mature stage), the **USA** (13% in Mature stage) and **Mexico** (12% in Mature stage) demonstrate low levels of readiness compared to the global average.

In Asia-Pacific, organizations in **Indonesia** (39% in Mature stage), the **Philippines**, and **Thailand** (27% each in Mature stage) top the chart both regionally and globally. On the other hand, companies in richer countries like **Japan** (5% in Mature stage) and **South Korea** (7% in Mature stage) are languishing at the bottom.

Markets most mature in their overall cybersecurity readiness

Mature stage



This variance could be largely explained by the fact that companies in emerging markets started their digitization journeys more recently compared to their peers in developed markets. That means many of these companies do not have legacy systems holding them back, making it relatively easier to deploy and integrate security solutions across their entire IT infrastructure. While awareness of security risks and their impact on business has never been higher, this finding highlights that 'tech debt' continues to be a major driver of the readiness gap.

This trend is not seen across Europe, though, where companies are lagging the global average on readiness.

In almost all countries less than 10% of companies are deemed mature enough to tackle today's cybersecurity issues. The **UK** and **Germany** are two exceptions, with 17% and 11% companies in a mature state of readiness respectively.

Readiness by Size and Industry

Readiness varies across company sizes in an interesting way. The data shows that globally mid-sized firms of between 250 and 1,000 employees are best prepared, with over 19% of such firms at a mature stage of overall readiness compared to 17% of larger businesses (1,000+ employees). This suggests that while larger organizations may have bigger budgets, they typically require more complex deployments, which can take longer to implement.

Smaller organizations are the least well-prepared with just 10% being mature in their readiness. While this is not surprising, it is an area of concern, as small companies falling below this 'security poverty line' bring wide-reaching externalities – they're increasingly part of supply chains of larger organizations, making them an attractive target for malicious actors. In today's hyper-connected world, it is critical to ensure there are no weak links that bad actors can exploit.

Of course, readiness is also dependent on the type of industry in which our respondents work in. Those in sectors with the most to lose tend to have more companies in the Mature state of readiness, including healthcare (18%) and financial services (19%). However, it is retail, with 21% of organizations in the Mature category, that comes out on top. This likely reflects the substantial number of cyberattacks this industry has faced over the years, as bad actors regularly target the personal and financial data held by these organizations.

Closing the Cybersecurity Readiness Gap – Our Global Security Resilience Imperative

While the cybersecurity readiness gap may be alarmingly large, businesses are not standing still.

Security leaders are aware of the risks and are keen to invest in their cybersecurity readiness: 86% of organizations have plans to increase their cybersecurity budget by more than 10% over the next 12 months. 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.

As these companies invest in their cybersecurity readiness, confidence in their ability to stay resilient will improve. Of the companies that were ranked Mature, 53% said they were 'very confident' in the ability to stay resilient against potential cyberattacks in the next 12 to 24 months. On the other hand, only 30% of companies in the Beginner stage and 34% in the Formative stage said the same.

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 the 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.

Benchmarking Readiness

While most of us are broadly aware of the increased security risks brought about by the move to hybrid working, what isn't widely understood is how ready organizations are to face those risks.

Cisco's *Cybersecurity Readiness Index* is a new way of assessing how ready businesses are.

It is sourced from a double-blind survey of 6,700 private sector cybersecurity leaders in 27 global markets. 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.

We asked respondents whether their companies had solutions in place to meet the challenges of each pillar, and how far along they were towards full deployment.

The data was then organized and categorized into a state of readiness, where respondents were ranked from **Beginner**, to **Formative**, **Progressive**, and finally **Mature** based on the weighted scores of each pillar reflecting their importance: network (25%); identity (20%); devices (20%); data (20%); and application workloads (15%).

A fuller explanation of the methodology can be found at the end of this report.

Identity

In the hybrid work environment, it is critical for companies to be able to verify the identity of everyone who tries to access network resources and information. One can argue that this is the first line of defence from a security perspective.

Devices

There are two aspects to this. First are the devices that employees use to log on to a company network. These can be both official and personal. Second are other devices within the infrastructure – ranging from security cameras to smart printers, which are all connected to the network. Companies need capabilities to verify these devices and protect them from being accessed by bad actors.

Network

In today's way of working, the network lies at the heart of a comprehensive approach to security given that people, devices, data, and applications all move across it. Safeguarding the network from malicious actors, insider threats, and third-party risks is critical to the viability of the company.

Application Workloads

As companies move some or all of their operations to the cloud, they are also experiencing a shift in the way they manage and deploy applications. From containerization to serverless architectures, and microservices, protecting application workloads is crucial in today's digital landscape. Attacks against these platforms and services can lead to sensitive data breaches, loss of productivity, and irreparable damage to an organization's reputation.

Data

Often described as 'new currency,' data has emerged as one of the most valuable assets for businesses. It is critical for organizations to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing amount of sensitive information being stored and shared electronically, robust security capabilities and measures are foundational to achieving this protection.

Nearly half of our respondents (47%) and their organizations fall into the Formative category, where they have taken some of the much-needed steps to protect themselves but **cannot be classified as ready to meet the challenges** of our new hybrid world.

Based on the overall score, organizations are categorized into one of four stages of readiness:

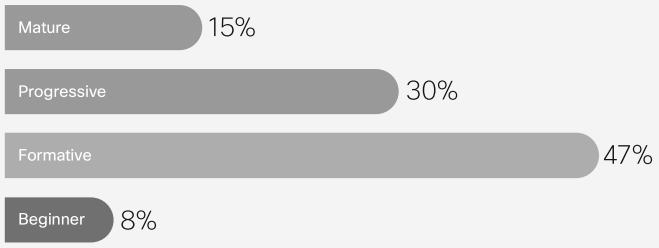
- **Beginner (Less than 10):** Organizations at the initial stages of deployment of solutions.
- **Formative (11 – 44):** Organizations that have some level of deployment but performing below average on cybersecurity readiness.
- **Progressive (45 – 75):** Organizations with considerable level of deployment and performing above average on cybersecurity readiness.
- **Mature (76 and higher):** Organizations that have achieved advanced stages of deployment and are most ready to address security risks.

Looking at the overall picture, nearly half of our respondents (47%) and their organizations fall into the Formative category, where they have taken some of the much-needed steps to protect themselves but cannot be classified as ready to meet the challenges of our new hybrid world. Progressives form the next largest cohort at 30%.

Only 15% fall into the Mature category, with a high level of readiness. Less than one in ten (8%) are in the Beginner category, representing the first step on the readiness ladder.

This report represents the first study of its kind and provides a comprehensive cybersecurity readiness assessment for companies across 27 markets globally.

Overall cybersecurity readiness of organizations globally



Protecting Identity

Traditionally, cybersecurity operations focus on creating a strong perimeter to keep out threats. The assumption being that anyone who was 'inside the wire' was authorized to be there. However, in the hybrid working model, data can be spread across limitless services, devices, applications, and users, making traditional perimeter approaches inadequate.

This calls for a new security strategy where no-one and nothing is trusted until their identity has been proactively verified. Our research underlines the challenge: a quarter (24%) of all respondents ranked Identity Management as the number one risk for cyberattacks.

For years, companies have relied on identity management solutions like Data Stores, which are a storage of things like identity of a person, their username, and their password. A person uses these to login, and if they match, they are granted entry. However, as companies have moved to remote and hybrid work arrangements, many have started to add a second layer of verification. These are Integrated Identity and Access Management (IAM) solutions, such as Multifactor Authentication, where even when a user enters the right username and password combination, they are then given a second prompt to prove that they are who they say they are.

Given that identity management is ranked by our respondents as the number one risk, it is no surprise that 95% have implemented some kind of identity management solution, with IAM proving most popular, with two-thirds saying they have deployed these solutions.

Some companies are adding yet another layer of security to identity management – Privileged Access Management. This is where, even after the first two layers of identity verification, access is granted based on pre-assigned privileges, such as the user's role within the company, the

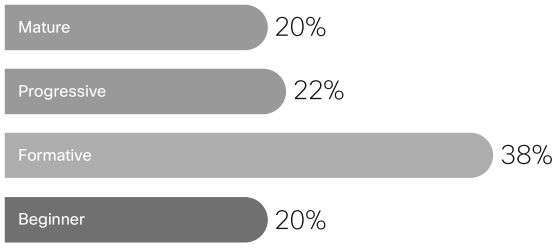
Given that identity management is ranked by our respondents as the number one risk, it is no surprise that **95% have implemented some kind of identity management solution**, with Integrated Identity and Access Management proving most popular.

device they are using to log in, and the location they are logging in from. The good news is that for all the identity management solutions – Traditional Data Stores, IAM and Privileged Access Management – our respondents are well progressed with most having fully deployed whichever solution they have decided to use.

However, it is of concern that for those that have not yet rolled out identity solutions, more than two thirds (69%) said they have no intention to do so. For those that do intend to roll out identity solutions, most will take from one to as many as five years to complete their implementation.

Overall, companies need to step up further to meet the challenge of identity verification. Despite the clear threat presented by identity management, most of our respondents are at the Formative (38%) or Beginner (20%) stage. Only 20% fall into the Mature category, with a further 22% in the Progressive segment. Surprisingly it is markets that are bigger and more mature that lag with the Netherlands (31%), France (35%) and Japan (50%) showing the highest percentage of Beginners.

Readiness to protect identity



Protecting Devices

Long gone are the days when employees accessed a corporate network from a single desktop PC. The need to access data on the move and in a variety of forms has created an explosion in the number of devices employees use. The pandemic has also added to the list of devices we all use regularly with cameras and microphones, for example, helping make video conferencing a better experience.

However, employee devices are not the only things accessing networks and data. Everything from soil moisture detectors to plant machinery, and even door security systems are connected to corporate networks, providing important and insightful data.

Whatever the device, it needs to be protected. We have seen significant data breaches in the past originating from unprotected devices.

For our respondents, protecting devices ranks third out of five in their list of risk potential, behind identity management and the network itself. It also seems to be less challenging for most with it ranking third on their list for difficulty.

Three quarters (73%) of our respondents have chosen to use enhanced anti-virus solutions as their key solution to protect devices. Building protections into the operating system, such as host controls, is another way organizations are protecting their devices, with 65% saying they have deployed this type of solution. Endpoint protection platforms – firewalls, malware, and process visibility etc. – rank third in the solutions companies have deployed.

However, there are two key trends to take note of. Firstly, the scale of deployment is partial. This is why, despite a high number of respondents saying they have these

Despite a high number of respondents saying they have these solutions in their posture, **more than half (56%) of the companies** are either at the **very start of their journey**, or only a **short way down the path**.

solutions in their posture, more than half (56%) of the companies are either at the very start of their journey, or only a short way down the path.

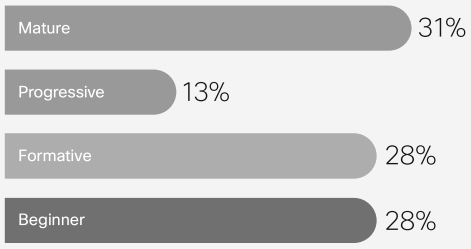
The second is that among those who do not have these solutions in their posture, device management does not seem to rank high in the list of cybersecurity priorities. Two thirds of these respondents said their organization has no plans at all to deploy a solution.

This shows that there is considerable work for many to do to ensure that devices do not become the vulnerable point in their cybersecurity strategy.

Japan is languishing at the bottom of the readiness league table with 56% of its companies falling into the Beginner category. New Zealand (45%) and South Korea (48%) do not fare much better and companies in all three countries should take note of the potential risks they run if they do not accelerate their device security strategy. The risks are particularly acute in Japan with 80% of companies still not planning to do so for at least 12 months and many (60%) are still to secure the budget for these programs.

By contrast, Indonesia is a long way in front of the readiness stakes with three out of five companies (59%) falling into the Mature category. Brazil (45%) and South Africa (44%) are other notable performers.

Readiness to protect devices



Protecting Networks

Globally, cyberattacks are on the rise. From telecoms to technology organizations and retailers, attacks have left networks vulnerable to exploitation. The result: billions of data sets have been exposed across the world.

At the last count, there had been more than 4,000 publicly disclosed data breaches[1] in the first three quarters of 2022 alone – a significant increase on the previous year. And the likelihood is that this is just the tip of the iceberg – with thousands more data breaches taking place in less well-known organizations.

Today's 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. The growth of cloud strategies – a bedrock of hybrid working – means that employees need to be able to roam across multiple networks throughout their day, rendering the network more vulnerable to cyberattacks.

Fortunately, our respondents recognize the risk; network protection ranks second in the list of their top five priorities.

Most have opted to use firewalls with built-in Intrusion Prevention Systems (IPS). More than two-thirds (69%) of firms in our survey said they had deployed this capability, with network segmentation policies based on identity ranking number two (61% said they have deployed this), and Network Behavior Anomaly detection tools close behind at 60%. Packet Capture and Sensor Tools, though, come a distant fourth at 31%.

However, the issue is that the scale of deployment is not keeping pace. Of those companies that have firewalls with built-in IPS, only 56% have fully deployed, and only 64% of companies have fully deployed network segmentation policies.

1. https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022

Regardless of where companies sit in their deployment, and which technology they use, there are some very real issues highlighted by our index which shows that despite companies rating network protection as their number two priority, most (56%) are either in the Formative or Beginner category and just 19% sit in the Mature category – the most advanced state of readiness.

This should be a clear signal to CISOs, CTOs and even CEOs that more work needs to be done to ensure organizations are better prepared to protect their networks.

Despite companies rating **network protection as their number two priority, most (56%) are either in the Formative or Beginner category** and just 19% sit in the Mature category.

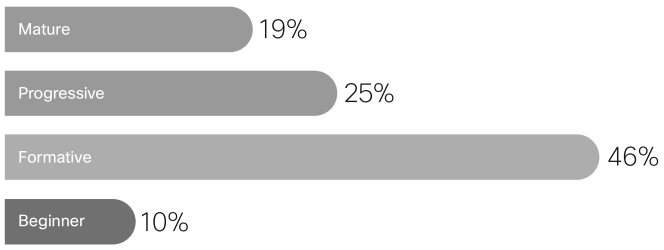
The problem is most acute in Japan where 82% of businesses fall into the least prepared categories. Hong Kong and Italy are not too far behind with 72% in the Formative or Beginner classification.

By contrast, some of the less developed nations in our research are most ready to protect their network. Perhaps this stems from the recognition that failing to protect their networks presents an existential threat. Whatever the trigger, though, Indonesia tops the readiness rankings with seven in ten (69%) falling into the top two categories. Thailand is second best prepared with six in ten (60%) ready to meet the threat.

One of the things that companies need to consider is that as business models move from static to dynamic, and hybrid work becomes the norm, network security must keep up. They need to look at novel approaches such as Secure Access Service Edge (SASE) to be adequately prepared to tackle the risks these shifts present.

SASE combines traditional network security functions with software-defined wide-area networking (SD-WAN) capabilities. It allows organizations to provide secure and reliable access to cloud-based applications and services for remote workers, regardless of their location. SASE also allows organizations to implement security policies that are specific to the user, device, and application, rather than just the network. The survey did show positive signs that companies are likely to continue to improve on this front. Among the companies that are still deploying network security solutions, half (50%) said they are planning to roll them out within the next 12 months.

Readiness to protect networks



Protecting Application Workloads

As we have already seen, the move to hybrid work and the proliferation of devices has made cybersecurity exponentially more complex. This, however, is only part of the story in our post-COVID world.

Businesses have come to rely heavily on applications, particularly so over the past couple of years. With the increased expectations that end users now have for always-on, secure, and exceptional experiences, organizations are under pressure to accelerate their digital transformation projects. Hundreds of thousands of organizations across the world are building, modernizing, and deploying all types of business-critical applications including traditional/on-premises, as well as modern, distributed cloud-native solutions.

In recent years, the pace of growth for applications has been phenomenal, and it will increase exponentially in the coming years. International Data Corporation (IDC) projects that 750 million cloud-native applications will be created globally by 2025[2].

While this has great benefits, it does present a new layer of risk for companies. The shift to modern, distributed applications can leave organizations more vulnerable due to an ever-expanding attack surface. According to latest research by Cisco AppDynamics, 78% of IT professionals globally feel that their organization is vulnerable to a multi-staged security attack that would affect the full application stack over the next 12 months[3].

Security teams have had to introduce a range of tools to their armories to protect against the additional threats presented in this more dynamic environment.

2. https://news.yahoo.com/idc-updates-future-digital-innovation-123000233.html
3. https://www.appdynamics.com/c/dam/r/appdynamics/2023/06-resources/08-ebook/AppDynamics_Application_Security_Report-1.pdf

Respondents to our survey have recognized the challenge, and 97% have deployed some kind of solution to protect application workloads. 66% have opted to use a host software firewall but endpoint protection was a close second with 64% of organizations choosing this to protect themselves. Less popular are application-centric protection tools (55%), and data loss prevention software (DLP) with just over a third choosing this route (34%), and visibility and forensic tools ranked fifth.

While host software firewalls proved to be the number one choice for most firms, only two-thirds (67%) have fully deployed the solution. Much of the rest are in the middle of deployment with 6% saying they have either just started deployment, or not yet begun.

Deployment of endpoint protection tools is even further behind with a little over half (57%) fully deployed and 35% presently deploying.

While 97% of respondents have rolled out application protection solutions, **most are not yet ready to meet the challenges ahead**.

The good news for nervous CEOs and those responsible for governance is that most respondents (88%) plan to deploy application protection solutions within 24 months. Although there are a worrying number of laggards with 12% expecting it will take three to five years, a substantial number of the delayed deployments are hamstrung by budgets, with only just over a third (39%) having agreed or allocated the necessary funds.

Less good news for worried CEOs is that, looking across all our respondents, two-thirds (65%) fall into the Formative or Beginner category of readiness. This means their organizations are either low (14%) or below average (51%) performers when it comes to readiness to protect an organization's application infrastructure.

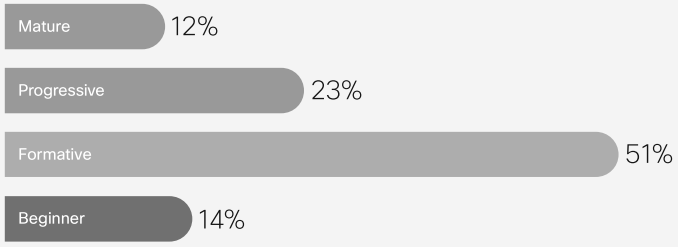
In short, it means that while 97% of respondents have rolled out application protection solutions, most are not yet ready to meet the challenges ahead.

Sadly, Japan again leads the way in countries less prepared to meet the challenge in this area of cybersecurity with half of respondents (47%) falling into the Formative category and a huge 39% in the Beginner grouping.

While Hong Kong and France fare better, they still rank 26th and 25th respectively in terms of readiness to repel attacks on application workloads. 81% of Hong Kong's respondents fall into the bottom half of preparedness while more than seven out of ten (77%) of organizations in France are low or below average performers.

As companies plan to take the next steps in readiness on this front, they should keep in mind that speed and coordination are paramount when dealing with application security risks. Bad actors can take advantage of gaps and delays between siloed security and application teams, resulting in costly and damaging consequences.

Readiness to protect application workloads



Protecting Data

Billions of datasets were stolen as a result of cybersecurity breaches in 2022, according to industry estimates.

For many affected, these hacks are an inconvenience resulting in wasted time changing personal details, passwords and so on. For businesses, the impact of data leaks can be highly significant. Not only do firms spend significant time on resolving the breach and enacting disaster recovery plans, but there are also major implications once the initial crisis is over. Regulators often want to understand the full extent of the incident and there can be punitive fines for firms that have not taken the right steps. Brand reputation can take years to recover for firms that have not acted properly to put in place expected cybersecurity mitigation programmes.

Our respondents seem to understand these implications and 98% say their organizations have solutions in place to protect data properly. Most have chosen either to encrypt data or to ensure that they are able to backup and recover lost data. More than two-thirds of firms (67%) have chosen these solutions for this pillar of protection.

Identification and classification with data leak protection is applied by 55% of organizations, while host IPS and protection tools provide a way forward for 41%.

The good news, bearing in mind the consequences of lost data, is that 94% have either fully or partially deployed encryption tools – which is the number one choice of most firms – while 92% have either completed or are on the road to completing the rollout of backup and recovery tools.

Identification and classification with DLP are a little behind on deployment, with just 55% fully deployed, while that number is 61% for host IPS and protection tools.

The **critical nature of data protection** explains why **the Mature and Progressive categories account for half** (50%) of the respondents in our survey.

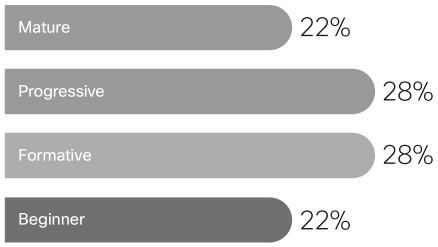
There is evidence that teams at many organizations still believe they need to do more to protect data with most that have not yet deployed solutions saying that they are planning rollouts. Of these, backup and recovery tools are the most popular with nearly half (48%) of the stragglers planning to deploy this solution.

There are some challenges over timelines, however, with 57% of respondents likely to wait more than 12 months before beginning their deployments. This stems from a lack of budgets with more than half (56%) not yet having agreed funding.

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.

As we look at the readiness data by country, Indonesia again leads the way in preparedness with 72% of all respondents in this market falling into either the Mature or Progressive stage. Not far behind is Brazil with just over two-thirds of respondents (68%) in either the high or above average performance category. South Africa is in third with 65% of respondents falling into the top two groups. At the other end of the readiness index is Japan with 77% of its respondents underperforming. South Korea is not far behind also with 74% in the bottom two categories.

Readiness to protect data



Industry and Size Matters

As we look at the industries that are most ready for the challenges ahead, they tend to be dominated by those with most to lose from cybersecurity incidents, and most to gain from keeping threats at bay. Healthcare, with the enormous challenge of keeping patient records safe, has the third highest number of organizations in the Mature category (18%) while Financial Services comes in second at 19%.

Retail comes out top with 21% of organizations in the **Mature category**.

Retail comes out top with 21% of organizations in the Mature category. This reflects the cybersecurity challenges the industry has seen over the last several years, and the pressure regulators are applying to keep financial and personal data safe.

If we look at each of the five pillars of security protection, some other industries stand out in their readiness to protect specific areas of their operations. Travel Services is the most progressed among all industries in the protection of data, with 26% of organizations in the Mature category – a necessary step given the large amount of personal information they process each day for customers taking flights and booking accommodation. It is also the second most advanced in the protection of devices after Retail, followed by Manufacturing which comes in third with 35% of organizations at the Mature stage. This could be attributed to the large number of IoT devices deployed in these industries.

Surprisingly, Restaurant Services shows a high level of readiness when it comes to identity management, coming in at second place with 25% of organizations at the Mature

Surprisingly, it is **the mid-sized companies** – those of between 250 and 1,000 employees – that are **best prepared with more organizations in the Mature category** (19%) than their larger competitors.

stage, just after Retail. This reflects the business models of many casual dining chains which require restaurant managers at multiple locations to order through a central system, as well as report takings and manage staff.

At the other end of the scale is Transportation where a little over 16% of organizations fall into the Beginner category. This is somewhat surprising given it forms part of a country's critical infrastructure but reflects the numerous legacy systems that tend to characterize this industry.

The Media and Communications sector ranks 17th on the readiness index (second to last), with 15% in the Beginner category. Given the power of media in today's world and the need to protect populations from bad actors, this is unexpected. We know media organizations are targeted, a recent example being the ransomware attack against the UK's Guardian in late December, 2022.

As we might expect there are differences in readiness depending on the size of the organization. Surprisingly, it is the mid-sized companies – those of between 250 and 1,000 employees – that are best prepared with more organizations in the Mature category (19%) than their larger competitors, and more in the Progressive category (31%) too.

These organizations are in the sweet spot. Large enough to be able to commit the budgets needed to get themselves ready to fend off cybersecurity attacks and agile enough to be able to deploy without the bureaucracy of larger businesses.

It goes without saying, unfortunately, that smaller organizations – those of up to 250 employees – tend to be less ready with more than 50% of their respondents dropping into the underperforming, Formative category. What's more, small organizations show a greater disparity between the two ends of the readiness spectrum.

There are more Beginners than Mature organizations among smaller organizations in four out of the five pillars of security readiness. This is in contrast to larger organizations, which have more respondents at the Mature stage than the Beginner stage across almost all five pillars of security protection. In particular, while organizations of all sizes are most progressed in device protection, almost one third of smaller organizations (32%) are in the Beginner category, significantly more than those that are mature (27%). The disparity could be due to the diversity among companies of this size, which may comprise family businesses, professional services firms, tech start-ups and more – all with varying levels of knowhow. With small and medium enterprises representing about 90% of businesses and more than 50% of employment worldwide[4], more support is needed to help them ramp up their security readiness.

Industries most mature in their overall cybersecurity readiness

Mature stage

21% Retail

19% Financial Services

18% Healthcare

Industries at the start of their cybersecurity journey

Beginner stage

16% Transportation

16% Media and Communications

13% Personal Care and Services

4. Small and Medium Enterprises (SME) Finance, World Bank

Conclusion

Those charged with protecting their organizations are faced with a myriad of new challenges brought about by the once-in-a-generation effects of the global pandemic. Despite its immediate effect on the world of work being largely complete, the effects on IT infrastructure are still being felt – and nowhere more so than in the offices of CISOs who are faced with a complex web of problems.

In today's business environment, significant thought and effort needs to be given to how to protect identities, devices, network, data, and applications that operate dynamically. The five pillars of security all need to be protected and they need to work in harmony or else organizations face the risk of presenting a target of opportunity to bad actors.

The five pillars of security all need to be protected and they need to **work in harmony** or else organizations face the risk of presenting a target of opportunity to bad actors.

Our report finds that in all five areas, businesses across the world are making progress albeit some industries are further ahead than others.

Progress is not even across all five pillars. Identity Management – recognized as the most critical area by our respondents – still has room for improvement, with close to three in five respondents (58%) finding themselves in either the Formative or Beginner category. Nevertheless, 95% are at least at some stage of deployment with a solution.

Efforts to protect the network – a particularly significant area given it is the backbone of all IT infrastructures – faces a similar situation with over half (56%) of respondents at the lower end of the readiness spectrum. That indicates many are in the early stages of deploying solutions although the good news is that half of our respondents (50%) plan to finalize deployments within the next 12 months.

Protection of devices is the most advanced of all five pillars, with almost a third of organizations (31%) falling into the highest performing category of readiness. As with identity management and the network, the challenge is deployment, with more than half (56%) of companies at either the Formative or Beginner stage. On the bright side, though, 88% of organizations that have not yet deployed solutions plan to do so within the next two years.

Looking at how organizations protect application workloads, 97% have deployed some kind of solution with most opting to use a host software firewall. This pillar is the least well advanced - nearly two-thirds (64%) fall into the Formative or Beginner stage of readiness. This means they are either Beginners (14%) or below average (51%) performers when it comes to readiness to protect an organization's application infrastructure.

When it comes to protecting data, 98% of respondents told us they have solutions in place. Most (67%) have chosen to encrypt data or ensure that they are able to backup and recover lost data. A large majority (94%) have either partially or fully deployed these solutions. These positive responses are also reflected in the readiness index where Mature and Progressive categories account for exactly half (50%) of the respondents in our survey.

The picture, then, is largely positive.

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 cyberattack are so clear to see, readiness must be a priority for all organizations and deployment of solutions needs to be accelerated.

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