My Location, My Device:
Hybrid work's new cybersecurity challenge

The security challenges faced by CIOs with employees working from unregistered devices

Mexico edition

Global Executive Summary

A little over two years after the global pandemic forced organizations to adopt home working overnight, what began as a contingency measure has become business as usual. And it's no longer confined to the home. People can now work from any location, and they do: our survey finds that **some employees are using more than ten different networks to log in to work**. Work from Home (WFH) really has truly become Work from Anywhere (WFA).

The new way of working has created huge opportunities. But it also brought new challenges for IT teams, including the need to make sure people have the tools and support they need to do their jobs from wherever they choose to. Organizations have had to make difficult decisions, often at speed. In this new normal, companies need to keep their employees connected everywhere, while limiting the security risks. And as the trends highlighted below show, it is not an easy task.

Cybersecurity is a huge concern

A massive **82%** of the security leaders we spoke to globally believe cybersecurity incidents are likely to disrupt their businesses over the next 12-24 months. As a result, they are gearing up to protect themselves from internal and external threats, **with 86% saying their organization plans to increase its cybersecurity budget** by at least 10% over the next 12 months.

The threat is real (and costly)

Nearly six out of 10 interviewees told us they had experienced a cybersecurity incident in the past 12 months. **Malware**, **phishing**, and **data leaks** are the top attack vectors for these breaches. The incidents cost **71%** of organizations affected at least US$100,000, with **41%** saying the overall cost was US$500,000 or more.

Work via unregistered devices is on the rise

The move to hybrid work is adding a new layer of risk and increasing the challenges for security professionals to tackle. Our survey finds that as people work from multiple locations, the use of unregistered devices to access work platforms is a major concern and growing risk.

- **84%** of respondents say their employees are logging in to work from unregistered devices
- **71%** say their employees are spending at least 10% of their day working this way
- **44%** say their employees are spending 20% of their day or more on an unregistered device logged on to the company network
- **84%** of global respondents say that remote working has increased the risk of cybersecurity incidents
- **84%** say unregistered devices are likely to cause a cybersecurity incident

With employees free to work from wherever they like, organizations need to ensure the networks they use are secure. But given that these networks might be anywhere from the local coffee shop to the supermarket, this poses a huge challenge for security teams.

There is an upside to all of this. The need to secure people, data and networks creates an enormous opportunity for increased public-private partnership. Governments all over the world are putting in place policies to curb cyber fraud and strengthen data protection. Organizations can invest in robust security solutions to make sure their customers have the best possible experience, and their employees can still enjoy the freedom to work from wherever they like, securely. We hope this study will provide readers with useful insights for navigating this tricky terrain.

Spotlight: Mexico

Among the security leaders interviewed in Mexico for this study, 40% said their organization experienced a cybersecurity incident over the past year, lower than the global average of 57%. Looking to the future, cybersecurity challenges are expected to increase with 76% of respondents believing an incident is likely to disrupt their organization within the next 24 months.

The study finds the most common types of attacks in Mexico are malware, data leaks, and phishing, with incidents costing 49% of organizations in the market at least US$100,000 and 23% at least US$500,000.

The increasing impact of hybrid working arrangements is adding another layer of cybersecurity challenges for companies in Mexico. According to the survey, 85% of respondents say their employees use at least two networks for logging into work, and 16% use more than five. This risk is recognized by security leaders with 79% in Mexico saying logging in remotely for hybrid work has increased the likelihood of cybersecurity incidents occurring.

The risks of hybrid work are being significantly amplified with the use of unregistered devices. Over eight in 10 (82%) Mexican respondents say their employees are using unregistered devices to log into work platforms, and 65% say their employees spend more than 10% of the day working from these.

On the bright side, with the challenges well recognized, 80% of Mexican security leaders expect their organization to increase its cybersecurity budget by more than 10% over the next year, and 93% expect upgrades to IT infrastructure within the next 24 months.

Security threats are causing disruptions

experienced a **cybersecurity incident** in the **past 12 months**

believe cybersecurity incidents are likely to **disrupt their organizations** in the next **12–24 months**

Top three types of incidents in past 12 months:

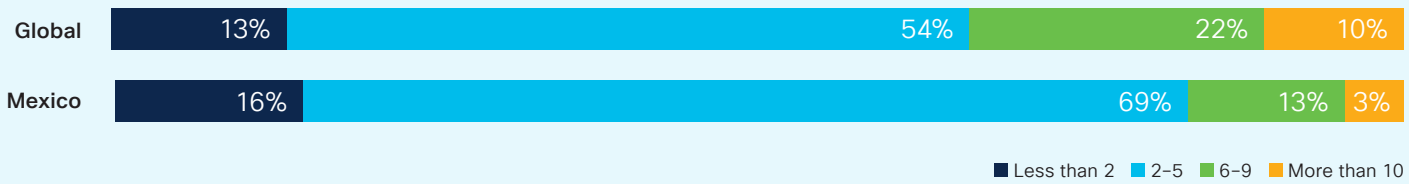
Global	Mexico
1. Malware 2. Phishing 3. Data Leaks	1. Malware 2. Data Leaks 3. Phishing

Cybersecurity incidents **cost impacted organizations** at least **US$100,000**.

Cybersecurity incidents **cost impacted organizations** at least **US$500,000**.

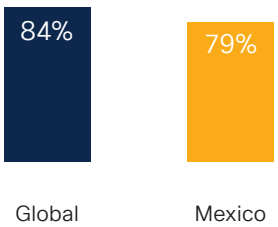
Hybrid and remote working is increasing the number of networks employees use

Average number of different networks employees now log on from for work in organizations globally:

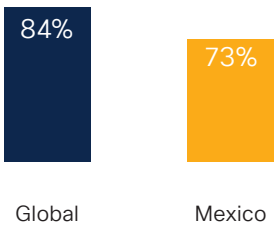


...and adding to cybersecurity risks

% of respondents who say **logging in remotely** as part of hybrid work has **increased cybersecurity risks** for their organization



% of respondents who say **unregistered devices** are likely to **cause cybersecurity incidents** for their organization



Organizations struggling to manage security risks posed by unregistered devices

Global	Mexico	
84%	82%	say their employees are logging onto their work platforms from unregistered devices.
71%	65%	say their employees spend more than 10% of the day working from unregistered devices.

Security spending rising as challenges mount

Global	Mexico	
86%	80%	say their organization plans to increase its cybersecurity budget by more than 10% over the next 12 months.
93%	93%	say their organization plans to upgrade or restructure its IT infrastructure to address cybersecurity challenges in the next 12-24 months.

What organizations need to do

Cisco recommends addressing four critical challenge areas while strategizing security of remote workers:

Unsecure connections

Compromised credentials

Limited or no visibility or control from the internet to the endpoint itself

Resource or time shortages

In a digital-first world, the ability to verify the identity of every user regardless of location is paramount. After verification, it's imperative to make sure the connection is secure, no matter the device.

Organizations must also be able to prevent and respond to threats from the cloud edge. Lastly, they should look for ways to increase automation, free up resources and focus security teams.

Building Security Resilience

Because threats are everywhere, we need to think about security differently. Stand-alone security strategies don't 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 what's coming down the road is anticipated so the organization can bounce back faster when a threat becomes real.

Most organizations are already thinking about resilience in their financial, operations, organizational, and supply chain practices. Security resilience cuts across all of them. No company should claim it can protect you from any threat any time. 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:

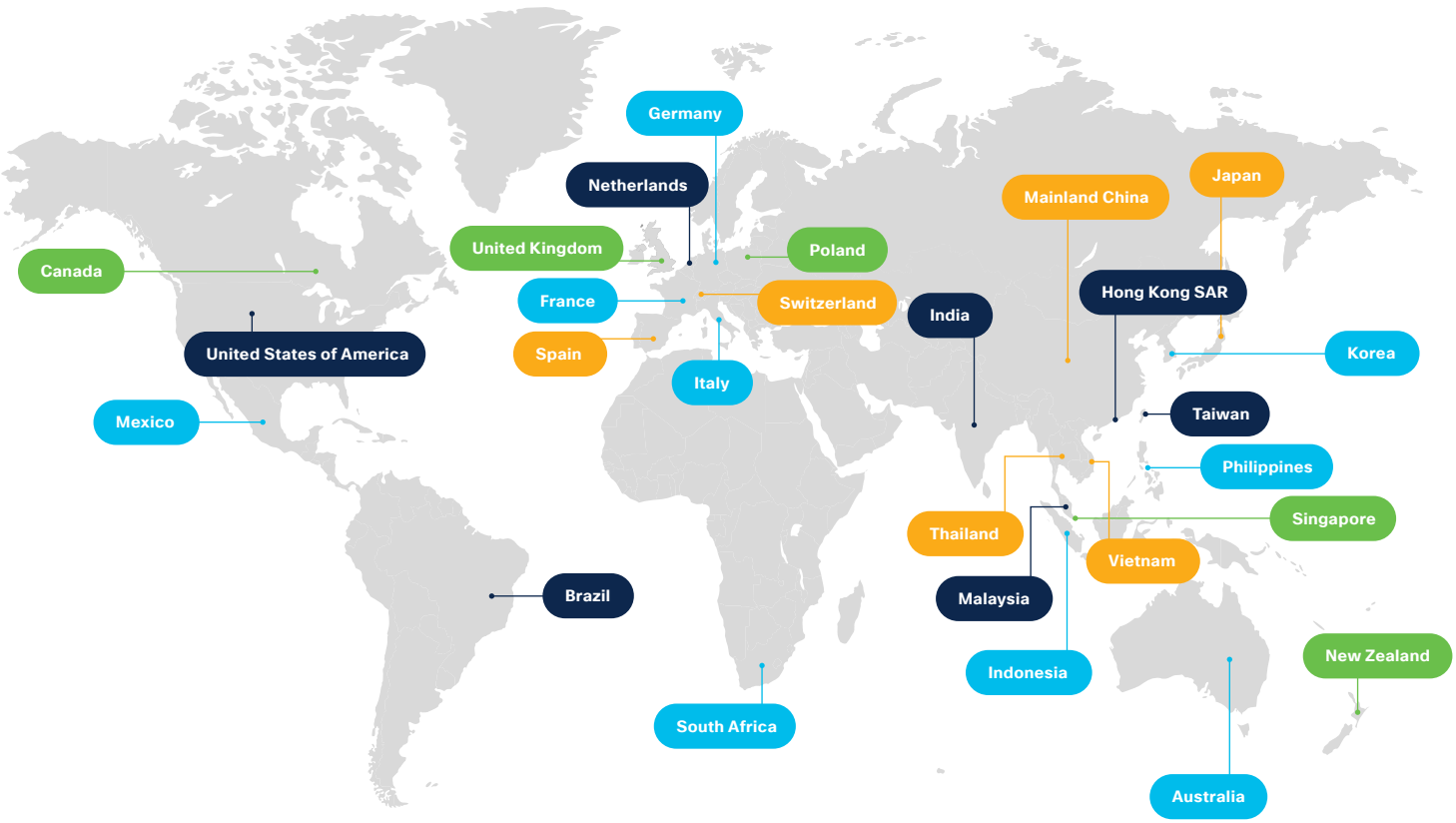
1. **Close the gaps in your system, so you have one open platform**
2. **See more and always be monitoring**
3. **Anticipate what's next using actionable intelligence**
4. **Prioritize what matters most**
5. **Automate your response so you can bounce back fast**

About the survey

The findings in this report are taken from an independent survey commissioned by Cisco of 6,700 business and IT leaders with cybersecurity responsibilities at organizations ranging from 10 to over 1,000 employees globally.

All interviews were conducted online during August and September 2022 with respondents representing every continent, excluding Antarctica.

The 27 markets included in the study are: Australia, Brazil, Canada, China, Hong Kong SAR, France, Germany, India, Indonesia, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Singapore, South Africa, South Korea, Spain, Switzerland, Taiwan, Thailand, United Kingdom, United States of America, Vietnam.




CISCO