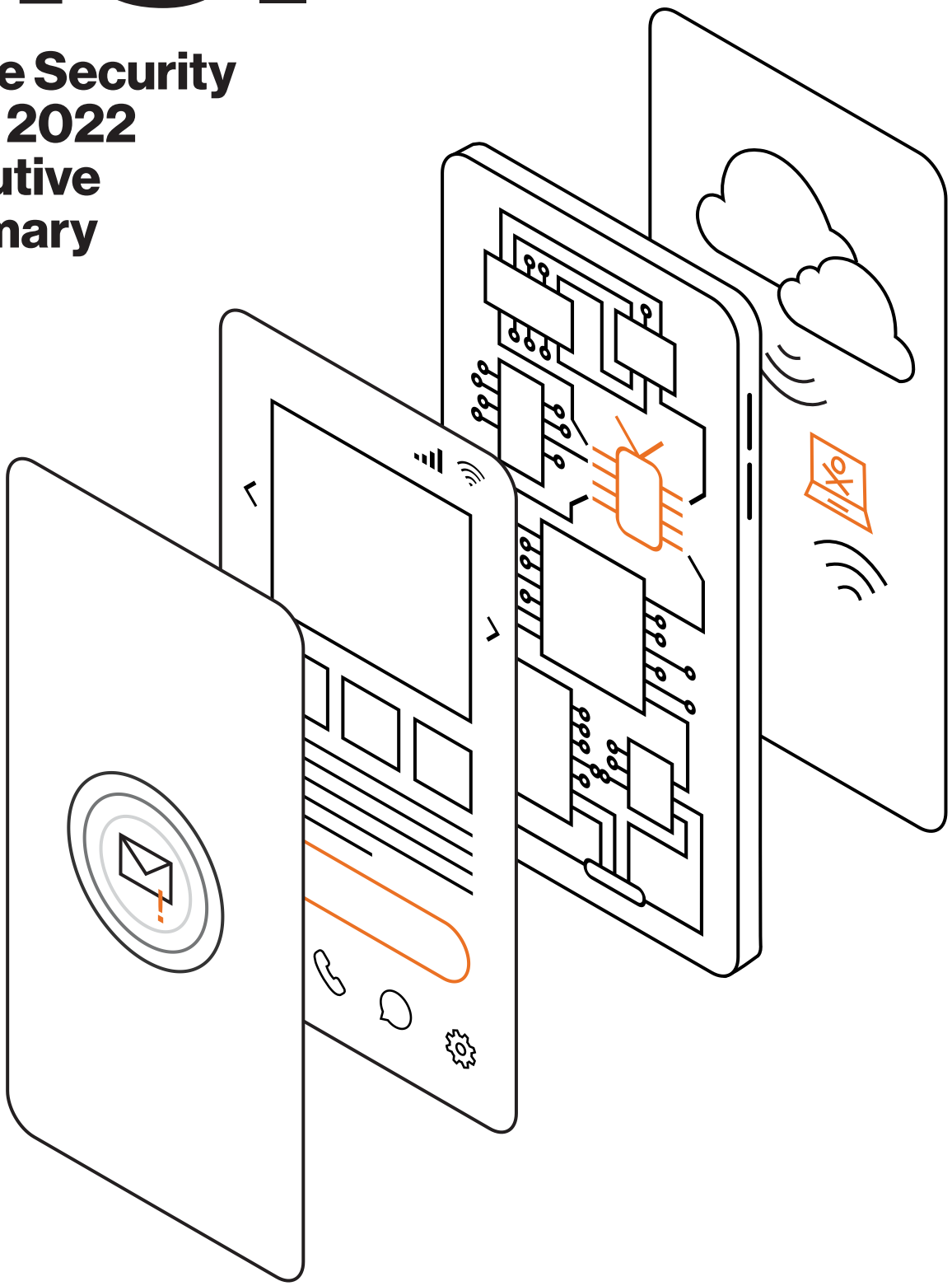
MSI

Mobile Security Index 2022 Executive Summary



Who should read this report?

We produced this fifth annual Verizon Mobile Security Index (MSI) to help security professionals, like chief information security officers (CISOs), assess their organization's mobile security environment and calibrate their defenses. While the report is packed with detail, there's also lots of information that would be interesting—and extremely relevant—to anybody involved in the specification, procurement or management of IT devices and services.

About this report

In April 2022, we commissioned an independent market research company to survey more than 600 people responsible for security strategy, policy and management. We also surveyed security practitioners and interviewed nine C-level experts in the field. And again this year we worked with several leaders in mobile device security: Absolute, Check Point, IBM, Ivanti, Jamf, Lookout, Netskope, Proofpoint and Thales. These contributors provided additional information, including incident and usage data.

We'd like to thank all our contributors for helping us to present a more complete picture of the threats that affect mobile devices and what is being done to mitigate them. This report wouldn't be possible without them.

Continue reading for the report's executive summary. For the full report, visit verizon.com/mobilesecurityindex.

The more things change ...

Normal?

Over the past few years lots has been written about "normal." There's been the "new normal" and the "next normal." In the immortal words of Inigo Montoya, "You keep using that word. I do not think it means what you think it means."

In most Western countries there simply isn't a preeminent working model in the way that there was a few decades ago. The pattern of sitting at the same desk five days a week has been falling apart for years; its demise was merely accelerated by the COVID-19 pandemic. Employees are increasingly asking for flexibility from their employers—and if their current employer isn't forthcoming, they may well move on. That has major implications for cybersecurity.

In April 2022, we commissioned an independent market research company to survey over 600 industry professionals responsible for security strategy, policy and management to provide their perspective on mobile security. Unless otherwise stated, the stats quoted in this summary are from this survey.

Where employees call "the office"

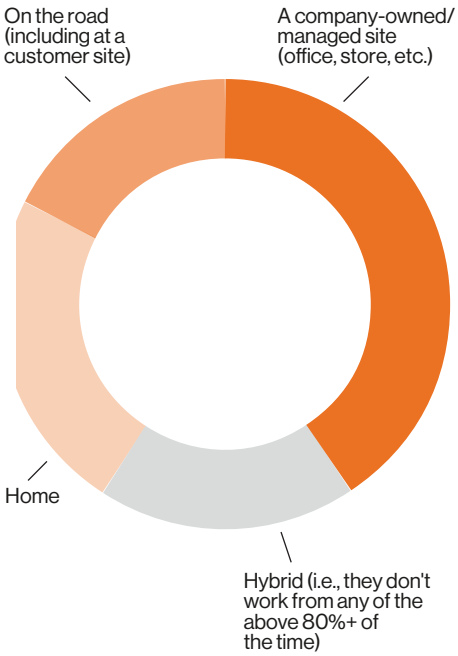
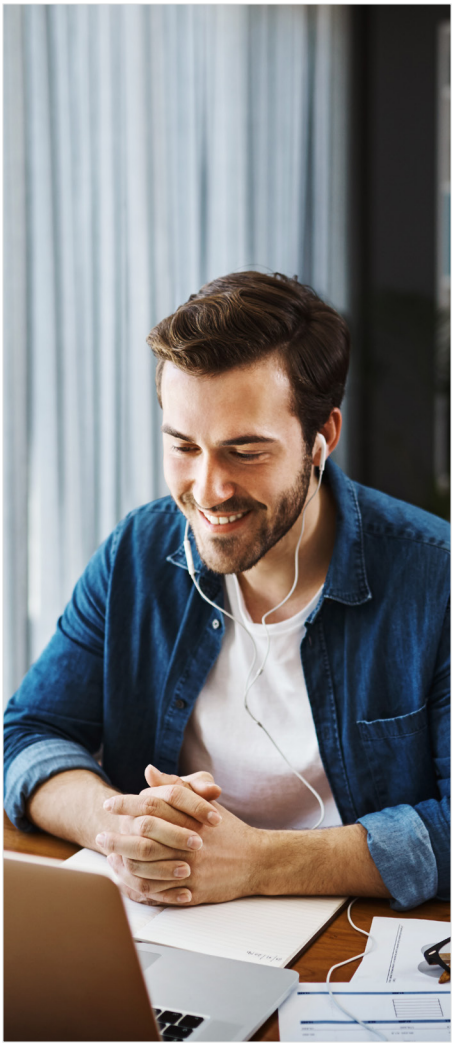


Figure 1. What proportion of your organization's staff work from each of these locations most (80% or more) of the time? [n=632]

According to research for the 2022 Verizon Mobile Security Index (MSI), on average, about two-fifths (40%) of employees work from the office most of the time (80% or more). About the same percentage (41%) work from home or "on the road" most of the time.



Flexibility is on everybody's agenda.

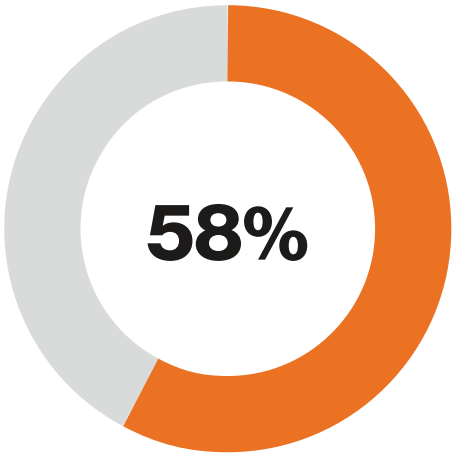
One thing is clear, the ability to be flexible—flexibility about flexibility—is going to be important in the future. And that's reflected in companies' increased use of—and reliance on—mobile devices.

In fact, many organizations see the ability to support flexible working options as key to their future strategy.

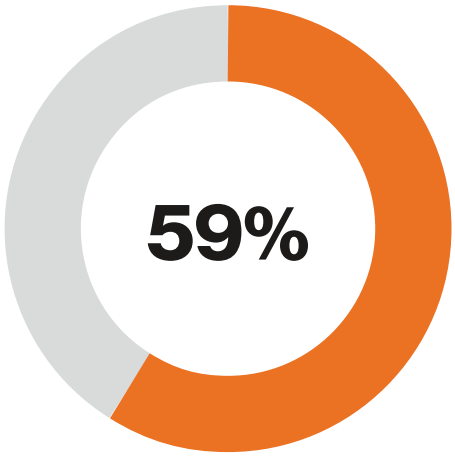
For many workers, mobile devices are no longer a secondary device. When asked how critical, on a 10-point scale, mobile devices were to the smooth running of their organization, 91% of respondents in our survey answered seven or above—and 78% answered eight or higher. The picture was very similar regardless of company operations (local, regional or global) or company size (small businesses to enterprise).

85%

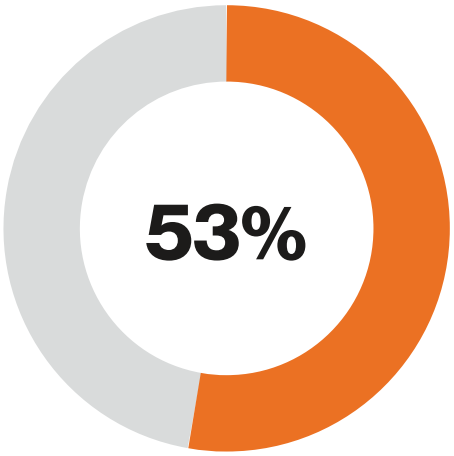
The vast majority of respondents said that flexibility in where they work and what devices they can use will be important to attracting the best new talent.



We have more users using mobile devices than 12 months ago.



Mobile users are doing more with their devices than 12 months ago.



Mobile devices have access to more sensitive data than a year ago.

... the more they stay the same.

Security compromises are up.

But as working practices have evolved, cybercriminals have been able to adapt, too. In some cases, the increase in remote work has given them a new advantage.

That at least partly explains the unprecedented increase, in the words of the Federal Bureau of Investigation (FBI), in cybercrime.

Growth in incidents and losses

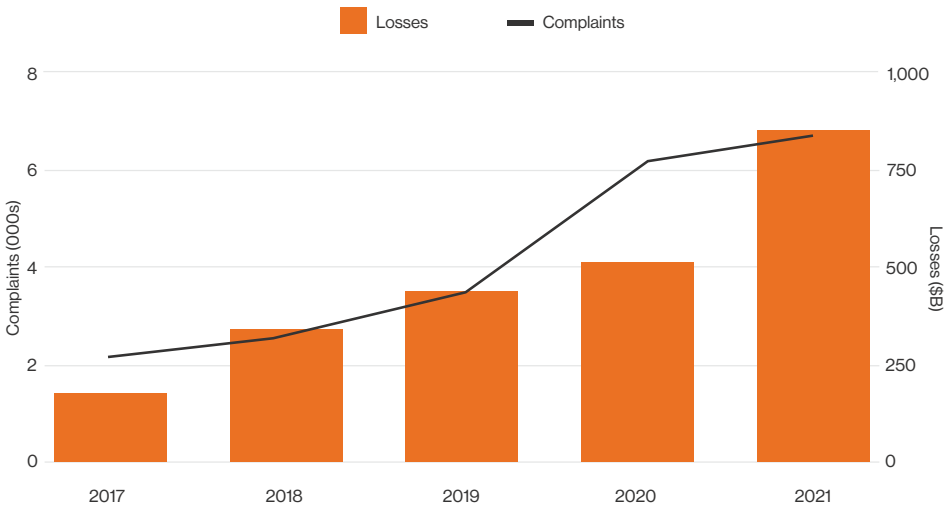


Figure 2. Reported incidents and losses, based on FBI data.[1]

Our MSI report found that 45% of companies had suffered downtime or data loss due to a mobile-related security compromise in the past 12 months. That's the highest seen in the five years that we've published the MSI—and 14% year-on-year growth since 2018.

79%

Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity.

"In 2021, America experienced an unprecedented increase in cyberattacks and malicious cyberactivity."

—2021 Internet Crime Report, FBI[2]

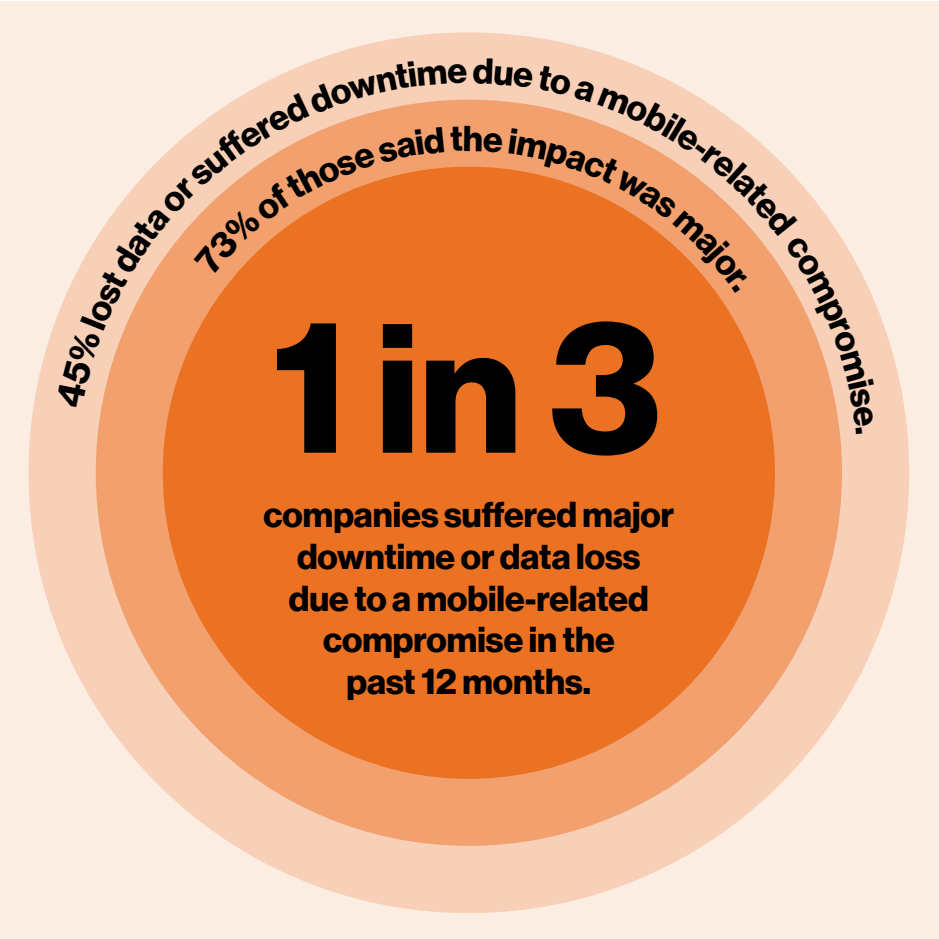
45%

Close to half of the companies that we surveyed said they had suffered a compromise involving a mobile device in the past 12 months. Companies with a global presence were even more likely to have been affected. More than three in five (61%) had been hit, compared to 43% of organizations with only a local presence.

1, 2 Internet Crime Report 2021, FBI, 2021.

The severity of attacks has grown.

Of those that had suffered a mobile-related compromise, 73% described the attack as major, and 42% said that it had lasting repercussions. With a lot more respondents saying that their company had experienced a mobile-related compromise, this means a lot more companies are facing major—and lasting—consequences.



47%

Nearly half of respondents that experienced a mobile-related compromise said that cloud-based systems/ apps were compromised as a consequence.

Companies are struggling.

Despite spending more, CISOs are feeling the pain.

Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity. And almost two in three chief information security officers (CISOs) across all regions agreed that remote working makes their organizations more vulnerable to cyberattacks.

According to a recent Proofpoint report, over half of CISOs across all regions agreed that targeted attacks on their organizations have increased since adopting mass hybrid working. Small organizations seem to have been affected most, with 59% of companies with 500 or fewer employees saying that their workforce has been targeted more since they implemented hybrid working. At the other end of the scale, only 48% of large enterprises (5,000 employees and above) said the same.[3]

Over three-quarters (77%) of MSI respondents said that their security spend had increased in the preceding year. More than a fifth said that it had increased significantly.

Change in security spend

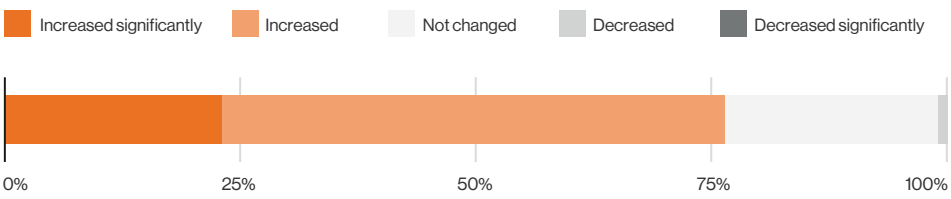


Figure 3. Year-over-year change in security spend. [n=632]

Top five factors driving increase in security spend

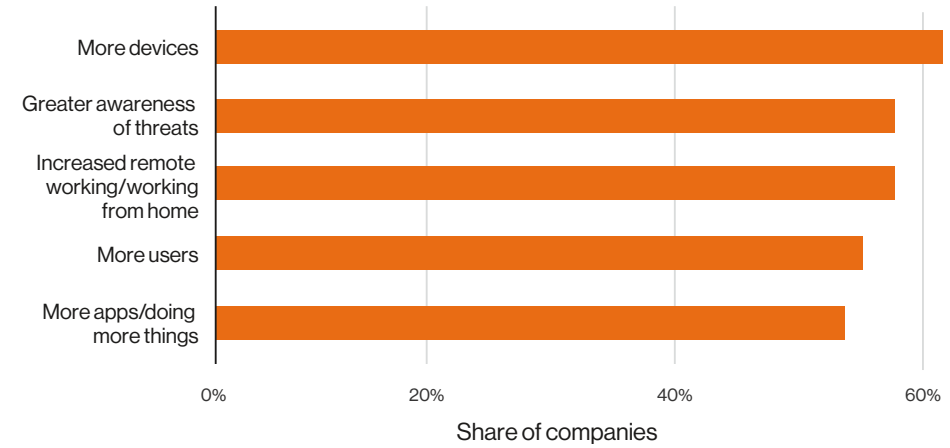
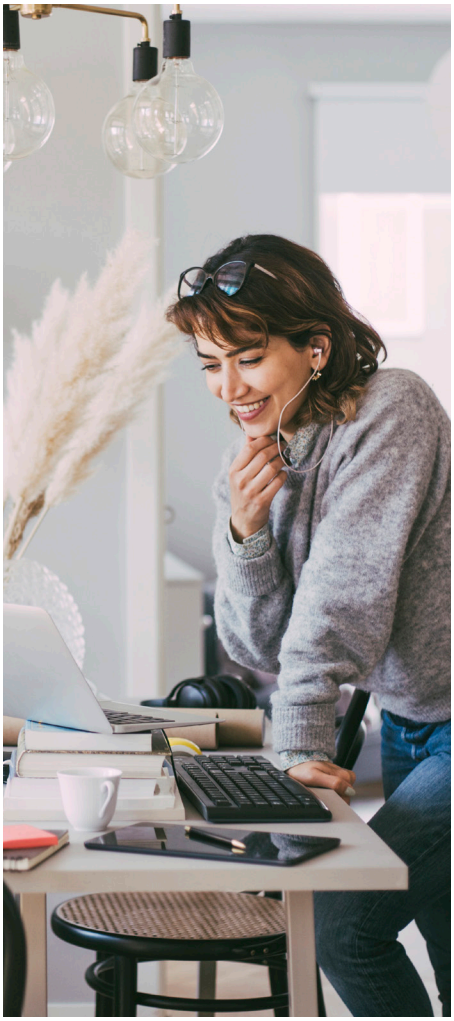


Figure 4. Top five factors that respondents said drove the increase in security spend that they saw in the preceding 12 months. [n=626]

22%

Over a fifth (22%) of IT leaders in an Absolute study said that their primary reason for wanting employees to work from the office is to maintain a better corporate security posture.[4]



3 2022 Voice of the CISO, Proofpoint, 2022.
4 The Future of Work, Absolute, 2022.

What you can do about it

The 2022 MSI report is packed full of insights into the threats facing mobile devices and how you can improve your organization's defenses.

We look at the most common attack methods and how attackers are evolving their techniques to adapt to greater awareness among both users and IT organizations. As well as insights from our own extensive survey and experts, the report features findings from contributors that include Absolute, Check Point, IBM, Ivanti, Jamf, Lookout, Netskope, Proofpoint and Thales. These companies provided additional information and data on mobile device usage and cybersecurity incidents.

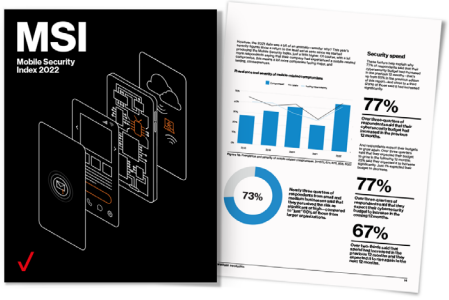
This year, we've included even more recommendations in the report. Six concise "how-to" guides offer expert advice to help tackle many of the common cybersecurity problems that businesses face, from implementing "bring-your-own-security" (BYOS) programs to building an incident response process. These will be particularly useful for organizations without a dedicated IT security function.

Whether you are a CISO looking for the latest insights about mobile threats or new to the field and seeking an easy-to-grasp introduction to mobile security, the MSI contains something for you.

82%

A large majority of respondents said that they had adopted or were actively considering adopting a Zero Trust approach to security.

The MSI is among Verizon's many cybersecurity reports. Take a look at some of our other publications.



2022 Mobile Security Index Report

Get mobile security experts' latest take on the most critical areas of focus.

Read the 2022 report >

2022 Data Breach Investigations Report

Learn when to engineer security solutions and when to rely on your security operations.

Read the 2022 report >

2022 Payment Security Report

Discover insights on upcoming changes to PCI DSS.

Read the 2022 report >

verizon