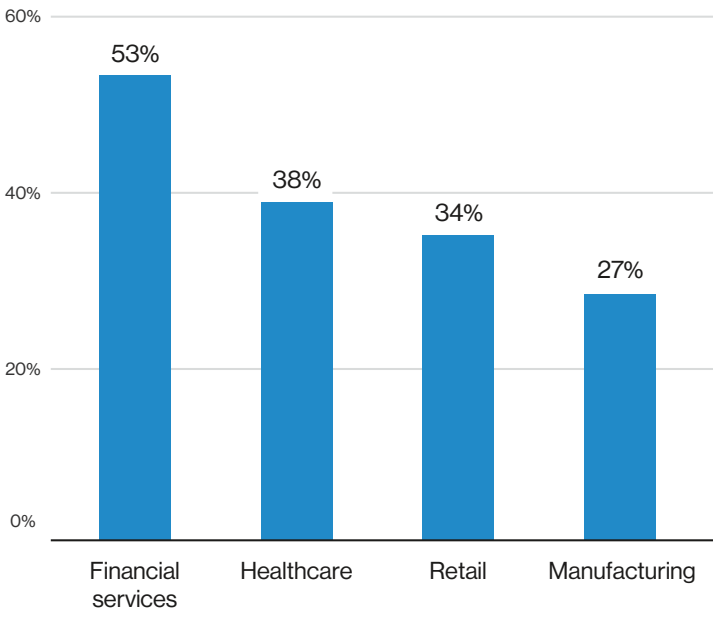
Mobile Security Index 2022: Enterprise

Spotlight

Key findings from extensive research into mobile-device security for the retail, manufacturing, healthcare and financial services sectors

Attacks are up.

Nearly half (45%) of all respondents to our Mobile Security Index (MSI) survey said their organization had experienced a mobile-related security incident that led to lost data or downtime in the past 12 months. That varied from "just" 27% of manufacturing companies to 53% of financial services organizations.



In this spotlight, we'll look at some of the variations between these industries, including the challenges they face and their approaches to improving mobile security.

Financial services

An enormous 70% of respondents from financial services organizations said they had sacrificed security for expediency—such as pressure from management to get a product or service to market quickly. And 58% said they'd done so for convenience—it was easier to go around the rules.

Those figures are even more alarming when you consider that our respondents were all involved in setting and enforcing IT security policy. The number of organizations affected may be even higher as some of those answering may not have all the information.

Of all the industries we studied, financial services organizations had the lowest share of employees—just 31% on average—working from the office most (over 80%) of the time. That helps explain why respondents from this sector rated the importance of mobile devices so highly—90% scored them as seven or higher on a ten-point scale, and 36% rated them the maximum 10, or "extremely critical." And 73% said that mobile devices were essential to being innovative and staying relevant to customers.

Largely in line with other industries, 78% of financial services companies said recent changes to working practices had adversely affected their cybersecurity. Only 45% rated their mobile-device security measures as very effective—which is unsurprising given that over half had suffered a mobile-related compromise in the previous 12 months.

This should be setting off alarm bells. Not only did 95% of respondents say their clients expect a reliable service and that even minutes of downtime could affect customer loyalty, most said they were bound by at least one regulatory framework. The most common frameworks were the Payment Card Industry Data Security Standard (PCI DSS) (76%), the General Data Protection Regulation (GDPR) (40%) and the Internet of Things Cybersecurity Improvement Act of 2020 (42%).

Healthcare

Survey respondents widely agreed that mobile devices and being able to access apps and data on the move are essential—and further, that mobility would be key to future innovation.

Those working in healthcare were no exception. Over three-quarters (76%) said telehealth offered a great opportunity to improve patient care. And half (50%) said it offered a great opportunity for growth.

A large majority (81%) said their organization had already enabled remote access to electronic patient records. This correlates quite closely with the 87% who said the highly confidential nature of their data made them a prime target for cybercriminals.

Despite this awareness, 51% of respondents from the healthcare sector said they'd sacrificed the security of mobile devices (including IoT devices) to "get the job done"—e.g., to meet a deadline or hit productivity targets. A further 17% said they'd come under pressure to do so but resisted. Uniquely, but hardly surprisingly, the most frequently given reason was dealing with the COVID-19 crisis.

Close to two out of five (38%) healthcare respondents said they'd experienced a mobile-related compromise in the previous 12 months. Half (50%) suffered loss of data as a consequence; over a third (37%) reported damage to their reputation, including loss of business; and the same number (37%) incurred regulatory penalties.

Driven by more users (cited by 65%), more devices (62%), increased remote working (59%) and greater awareness of threats (60%), the vast majority (81%) of healthcare organizations said their spend on mobile device defenses had increased in the past 12 months. A similar number (78%) expected their spend to increase in the following 12 months.

Healthcare respondents were significantly more likely (69%) to say they were struggling to reconcile disparate mobility demands from different areas of the business. And 79% said the need for employees to be able to access data quickly made it harder for them to implement effective security controls.

That helps explain why reducing burden on the IT team (e.g., automating tasks) (chosen by 55%) and integrating management of security of phones, tablets and laptops (chosen by 59%) were high on the list of objectives for increased investment.

Retail

Almost three-quarters of respondents working in retail said they'd come under pressure to sacrifice mobile security—and 52% had done so. Of those who admitted to having succumbed to the pressure, 57% said it was for expediency (e.g., pressure from management to get products or services to market quickly), and 36% attributed it to convenience (e.g., it was easier to go around company policy).

We've seen this many times before. When the pressure is on, security comes second—or worse. It doesn't have to be like this. But when asked what the objectives for their security spend were, fewer retail respondents listed reducing inconvenience to users and increasing productivity than any of the other options.

In our most recent survey, retail and hospitality firms were significantly less likely to report having suffered a mobile-related compromise. Just over a third (34%) said they'd suffered an incident that resulted in the loss of data or downtime in the past 12 months. That's much better than the 53% reported in the financial services industry and the 45% across all industries. But that's still one in three that know they were compromised—and we still believe that companies are under-reporting, given that many will report an attack without recording details of the devices involved. It would be recorded as, say, phishing, but not that it happened on a mobile device.

It's also important to note that five out of six (86%) retail respondents said they think mobile-device threats are growing more quickly than other threats.

Over two-fifths (44%) of those that did identify the involvement of a mobile device said they'd suffered damage to their reputation, including loss of business, because of the compromise. Bear in mind that 87% said that a security breach could have a lasting impact on customers' loyalty to their brand.

That would help explain why they are spending more on security. Close to three-quarters (72%) of retail respondents said their spend on mobile device security had increased in the previous 12 months. The most common reason stated was an increase in the number of devices (58%). Looking ahead, 76% expected their spend to increase in the coming year.

Manufacturing

Significantly more than half (58%) of respondents from the manufacturing industry said they depend on users being connected all the time. That's more than any other industry.

More than four-fifths (81%) of those working in manufacturing said they'd seen an increase in mobile-related threats in the previous 12 months. Almost a quarter (23%) said they'd seen a significant increase.

Over a quarter (27%) of manufacturing respondents said their company had experienced a security compromise involving a mobile device in the past 12 months. That's significantly lower than the other industries we looked at, but still substantial. If you were told that you had a 27% chance of being mugged in the next 12 months, you'd take precautions. Manufacturers should take the risks of being compromised seriously, too.

More than four-fifths (81%) of those that experienced a mobile-related compromise called the impact major. The consequences included the compromise of cloud-based systems/apps (52%), downtime (48%), loss of data (38%) and reputational damage (38%).

As with other industries, manufacturers are under pressure to transform their business, and that almost always involves a significant increase in the use of technology. More than four-fifths (81%) of manufacturing respondents said being able to take a future crisis in stride was key to their planning and investment. And 87% said the growing integration of operational technology (OT) and IT makes mobile device security more critical.

A massive 95% of manufacturing respondents said organizations need to take the security of mobile devices more seriously. That's not a surprise given that 79% said a security compromise could disrupt their supply chain, with serious financial implications. Considering the disruption of the last few years, that's the last thing manufacturers need right now.

It's no surprise then that 85% of manufacturers said their mobile-device security budget had increased in the previous 12 months. And 78% said they expected it to increase in the next 12 months. But despite those increases, only 79% said their anticipated budget for the following 12 months would be adequate to protect their employees, their intellectual property, and their owners' and stakeholders' interests.

Find out more.

The fifth edition of the Verizon Mobile Security Index is available now. It's based on a survey of over 600 professionals responsible for the procurement, management and security of mobile devices. In addition to data and insights from Verizon, the report features contributions from other leading cybersecurity practitioners, including Absolute, Check Point, IBM, Ivanti, Jamf, Lookout, Netskope, Proofpoint and Thales.

The 2022 report includes deep dives on key threats like phishing, ransomware and inappropriate use. It's also packed with actionable recommendations—from how to secure a bring-your-own-device (BYOD) setup to how to create an effective incident response program. The insights in this report, combined with the concise how-to guides, could help you transform your mobile device defenses and protect your users, your customers and your organization's reputation.

Read the full report at verizon.com/mobilesecurityindex