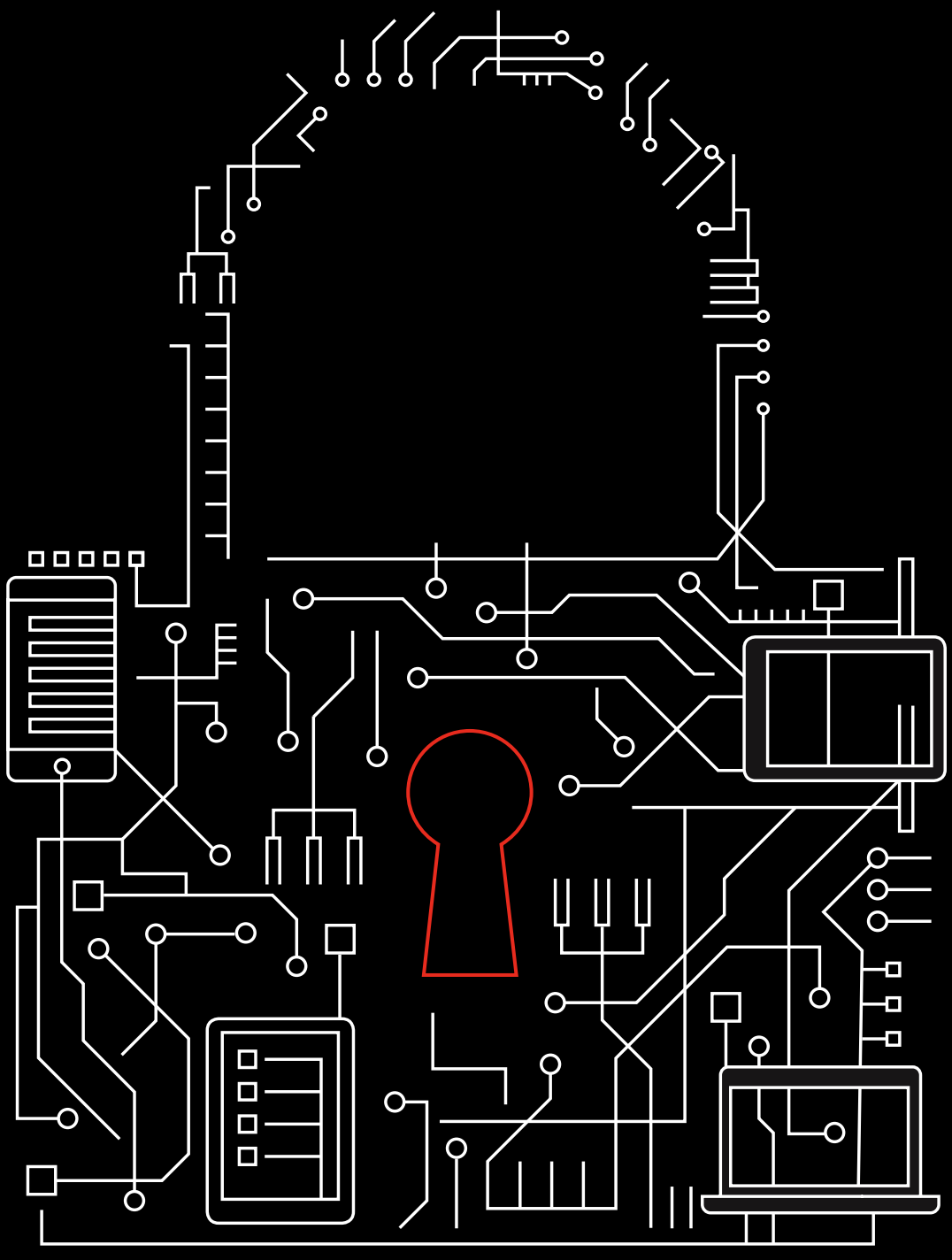
Mobile Security Index

2020 executive summary



verizon

Mobile security is critical for innovation.

Survival for the modern organization requires constant innovation, and today, that means mobile technology.

As part of the 2020 Mobile Security Index, we asked our survey respondents to rate how crucial mobile is to their business on a 10-point scale; 83% answered 8 or higher. That means that securing mobility is no longer optional, but crucial to securing future innovation and transformation. This is exacerbated by the facts that regulatory pressures are increasing and consumer and business customers are becoming more sensitive to how their data is protected.

Keeping ahead of bad actors and mal-innovation to deliver the experiences that consumers and employees expect is an ongoing challenge. Doing so successfully isn't just about the tools that you use; you also need an approach that puts mobile security right at the heart of your IT strategy.

Read on to boost your understanding of the state of mobile security and the threats facing organizations today.

54%

Fifty-four percent of companies were less confident about the security of their mobile devices than that of their other systems.

verizon

More organizations are falling victim.

What might be the most distressing result from this year's Mobile Security Index isn't necessarily surprising: The percentage of companies that have suffered a compromise continues to go up. In fact, since our first report in 2018, the percent of companies reporting a compromise has gone up 41%. Cyberattackers have been quick to find opportunities—they see the growing importance of mobility to organizations around the world and they know the value of the data that those mobile devices have access to.

To get a hold of your data, attackers are using old standbys like phishing and malware, as well as cunning new tricks. They're targeting every aspect of the mobile ecosystem: users, apps, devices and networks.

Companies that were compromised

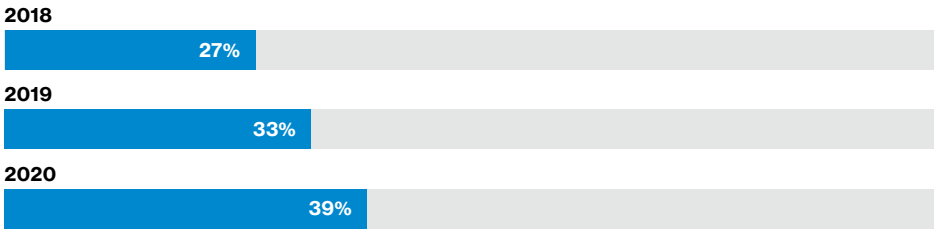


Figure 1. Has your organization experienced a security compromise involving mobile/Internet of Things (IoT) devices during the past year?

Users

Whether they deliberately break policy, inadvertently open up vulnerabilities or act in a malicious manner, users can present a security challenge. And attackers are finding increasingly innovative ways to exploit and manipulate your employees. Social engineering is one of the most powerful tools in the cybercriminal arsenal to do this.

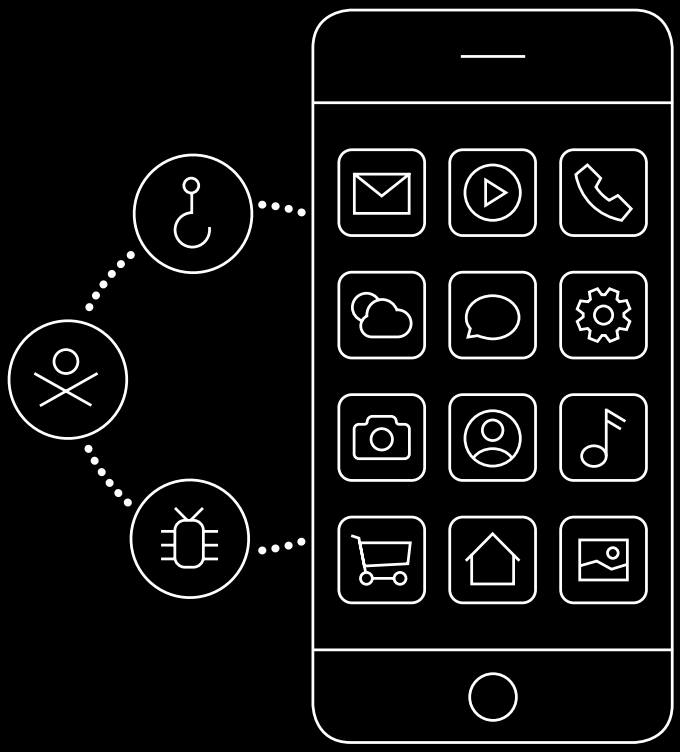
Phishing and business email compromise are two popular examples of social engineering, and for good reason. According to the U.S. Secret Service, which contributed to this year's report, the average loss from a bank robbery is about $3,000, while the average loss from a successful business-email compromise attack is nearly $130,000.[1]

There's no silver bullet for mobile security, but an acceptable use policy (AUP) is a key starting place to set organizational guidelines and improve employee knowledge of threats. A strong AUP will set criteria for appropriate and inappropriate websites; set expectations on acceptable data volumes; guide employees on compliance; and help keep your data safe. Unfortunately, we found 44% of respondents didn't have one at all.

15%

Fifteen percent of enterprise users (18% in the U.S.) encountered a mobile phishing link in Q3 2019.

Want help strengthening your AUP? Check out our AUP guide. ›



When the innovation award goes to the bad guys

In this year's research, we saw evidence of hackers sneaking malicious apps into official app stores and using elusive techniques like delayed triggers and custom fonts to obfuscate email content so it's not picked up by scanning software.

21%

Twenty-one percent of organizations that were compromised said that a rogue or unapproved application had contributed to the incident.

Apps

Malware and ransomware remain dangerous and all too common, but techniques like cryptojacking are becoming more frequent as well. Cryptojacking is when attackers use a compromised device to mine cryptocurrency such as Bitcoin. It not only drains the battery life of the device, but can also lead to downtime or other disruptions.

This year, 86% of organizations said they were concerned about malware. Yet many companies are not regulating which apps their employees are using—only 43% said that they limit their employees to using apps from an official app store or one owned by the company.

Devices

This year, our study looked at organizations ranging from those with fewer than 100 mobile devices to companies with 10,000 or more. And all of them were worried about the same types of device threats, from lost devices to operating system vulnerabilities. In fact, 83% of organizations were concerned about device loss or theft, and 20% of those felt that their defenses were inadequate. Organizations can use standard security features such as device encryption and remote wipe to help mitigate the risk.

Device operating systems are also a concern and often out of date. Almost half (49%) of enterprise devices are being used without any managed update policy.

Networks

The siren song of public Wi-Fi is snaring users and increasing risk for organizations. Twenty percent of organizations that suffered a mobile compromise said that a rogue or insecure Wi-Fi hotspot was involved.

According to Wandera, employees connect to an average of 24 Wi-Fi hotspots per week,[3] and Netmotion found that the average device connects to two or three insecure Wi-Fi hotspots per day.[4]

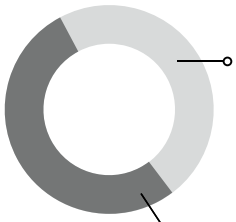
31%

Thirty-one percent of devices were found to harbor known threats, based on MobileIron data.[2]

2 to 3

The number of insecure Wi-Fi hotspots an average device connects to each day

Policy on public Wi-Fi



48%

Forty-eight percent of companies prohibited the use of public Wi-Fi.

52%

Fifty-two percent of companies either allowed the use of public Wi-Fi or had no policy.

Employee use of public Wi-Fi

72%

Seventy-two percent of all employees used public Wi-Fi.

Including 55% of employees who worked at companies that prohibit doing so.

28%

Twenty-eight percent of all employees didn't use public Wi-Fi.

Figure 2. Are your employees allowed to use public Wi-Fi (e.g., in a coffee shop or hotel) for performing work-related tasks? Do you ever personally use public Wi-Fi for work-related tasks?

Assessing the consequences

Surely, in this day and age, organizations understand the vital role mobility plays in an overall security architecture? Well, the evidence isn't so clear. Forty-three percent of organizations admitted to sacrificing mobile security to meet deadlines or productivity targets. And those that did were twice as likely to be compromised.

Why make such risky decisions? Speed (62%) and convenience (52%) topped the list of reasons respondents gave for sacrificing security. Profitability (46%) came in close behind. All of those are important business imperatives, but balance them against possibly doubling your likelihood of a compromise and the choice to sacrifice security becomes harder to justify.

Sacrifice and compromise

43%

Forty-three percent of companies sacrificed security.

39%

Thirty-nine percent of companies suffered a security compromise.

Figure 3. Has your organization experienced a security compromise involving mobile or IoT devices during the past year? Has your organization ever sacrificed the security of mobile devices (including IoT devices) to "get the job done"?

Those that were hit felt the pain.

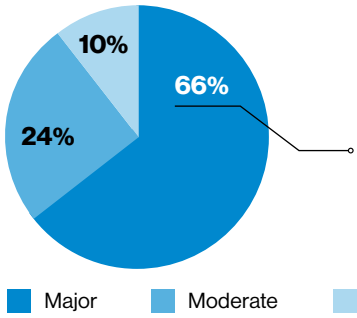
Sixty-six percent of organizations that suffered a compromise called the impact "major." Clean-up proved tricky for at least 37% of respondents, who said that the compromise that they experienced was difficult and expensive to remediate.

The effects of those compromises often stretched far beyond mobile devices as well, with immediate impacts including:

- Downtime (59%)
- Loss of data (56%)
- Regulatory penalties (29%)

If you think you don't need to worry too much about mobile security because your organization is small or your industry isn't a target, think again. We didn't find a single sector that hadn't suffered compromises, and victims ranged from organizations with fewer than 50 employees to those with more than 10,000.

Impact of being compromised



55%

Fifty-five percent of these companies said that the repercussions were lasting.

Figure 4. If your organization suffered a security compromise, how serious was the impact? If the compromise was major, did this involve lasting repercussions?

The cloud, IoT and the 5G future

The benefits of continued cloud adoption, Internet of Things (IoT) systems and 5G networks are enabling entirely new customer and employee experiences, and transforming business across all sectors. That is why this year's Mobile Security Index takes a look at each of these technologies and their impact on mobile security.

Cloud

The cloud's growing role in infrastructure cannot be overstated. Fifty-seven percent of companies said that over half the new business information they create or gather is stored in the cloud, and 84% said that their reliance on data stored in the cloud is growing. And yet, only about half (52%) of respondents said that they block the use of cloud apps when they're accessed from unknown networks.

IoT

We took a special look at IoT by identifying a subset of our respondents who were responsible for buying, managing and securing these devices and giving them a customized question set. We found that the challenges we saw in mobile were mirrored in the IoT environment. Nearly a third (31%) of IoT respondents admitted to having suffered a compromise involving an IoT device. As with mobile, cutting corners was partially to blame. Two-fifths (41%) admitted to having sacrificed IoT security to "get the job done" and this was shown to have consequences. Organizations using IoT that sacrificed security were 1.7 times as likely to have suffered a compromise involving an IoT device.

5G

With 5G, companies stand to benefit from exciting new interactive services, like augmented and virtual reality. 5G is also expected to accelerate developments in IoT applications, including connected vehicles, smart spaces and intelligent buildings. The ability to help secure these services and applications is a key part of 5G's underlying architecture.

The new security features and capabilities of 5G include:

- Better protection against unauthorized tracking and ID theft using subscription concealed identifiers (SUCIs) and globally unique temporary identifiers (5G GUTIs)
- Greater resilience against attacks through the use of using software-defined networking (SDN) and network function virtualization (NFV)
- Tailored security to support new devices and use cases
- Better protection from rogue base stations by using implicit keys and verification when using non-3GPP networks like Wi-Fi

What's driving change

Globally, governments continue to modify and increase protections and regulations concerning mobile security. Sixty-seven percent of organizations said that increased regulation had driven them to spend more on security as a whole.

Unfortunately, many companies only take mobile security seriously after things go wrong. We found that 43% of companies that had suffered a compromise were planning to significantly increase their mobile security spend in the coming year, compared to 17% of those that hadn't been compromised.

84%

Eighty-four percent of organizations said that their reliance on data stored in the cloud is growing.

31%

Thirty-one percent of IoT respondents admitted to having suffered a compromise involving an IoT device.

Those compromised were more likely to significantly increase spend.

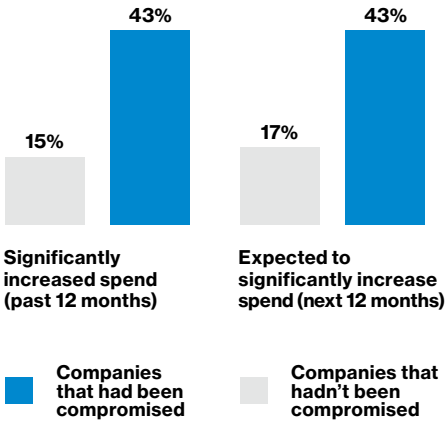


Figure 5. Change in mobile device security spend broken into those that had experienced a compromise and those that hadn't.

How to improve mobile security

Forty-five percent of organizations said that their defenses are falling behind attackers' capabilities. The Mobile Security Index 2020 can help you avoid becoming one of those organizations. This year, we have added interviews with experts who offer detailed suggestions on how to fine tune your security approach.

For those looking for the high-level view, here are some of our top tips for boosting mobile security:

Users:

- Establish a formal AUP that specifies responsibilities for bring-your-own-device users, what networks can be used and what apps users can install
- Adopt a security-first focus, give all employees regular training and make sure users know how to report anything suspicious
- Set and communicate a password policy covering strength, reuse and two-factor authentication

Apps:

- Restrict access to data on a need-to-know basis
- Limit employees to installing apps from vetted sources, and block those downloaded from the internet
- Ensure that all patches are installed promptly

Devices:

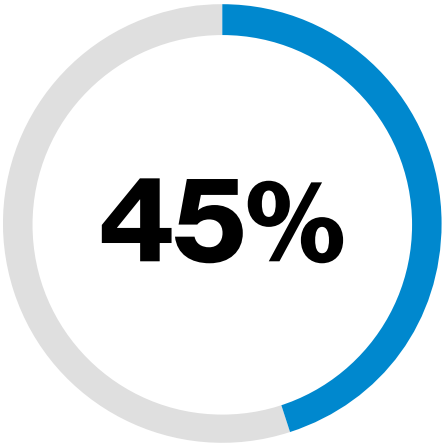
- Change all default and vendor-supplied passwords—and avoid reusing the same ones
- Implement policies to lock down and isolate vulnerable, infected and lost or stolen devices
- Use a mobile device management (MDM) solution to simplify patch management and enforce your AUP, including authentication policies
- Deploy mobile threat detection software to regularly scan devices for vulnerabilities

Networks:

- Encrypt all data sent over unsecured networks
- Educate users on the dangers of public Wi-Fi, and block the use of unknown or insecure Wi-Fi networks
- Consider adopting a zero-trust approach

Cloud services:

- Restrict the use of unvetted cloud apps, especially file-sharing ones
- Limit access to cloud services to devices using trusted networks or VPNs



Forty-five percent of organizations said that their defenses are falling behind attackers' capabilities.

Get the report. Get secure.

You've taken the first step to improving your mobile security. Take the next one by downloading the full Mobile Security Index (MSI) 2020 report. Effective, multilayered mobile security is within reach of organizations like yours, and we've built tools to help you get there.

MSI 2020 main report

The full Mobile Security Index 2020 report provides even more detailed statistics and analysis of the threats facing mobile devices. It includes interviews with security experts, including an FBI Unit Chief and Verizon's Chief Information Security Officer (CISO).

MSI 2020 security assessment tool

Our mobile security assessment allows you to compare your security to your peers surveyed for the 2020 MSI report and provides a custom report with pointers on how to improve your security.

MSI 2020 acceptable use policy guide

This interactive guide helps explain what makes up a strong AUP and provides tips on how to build or improve your own.

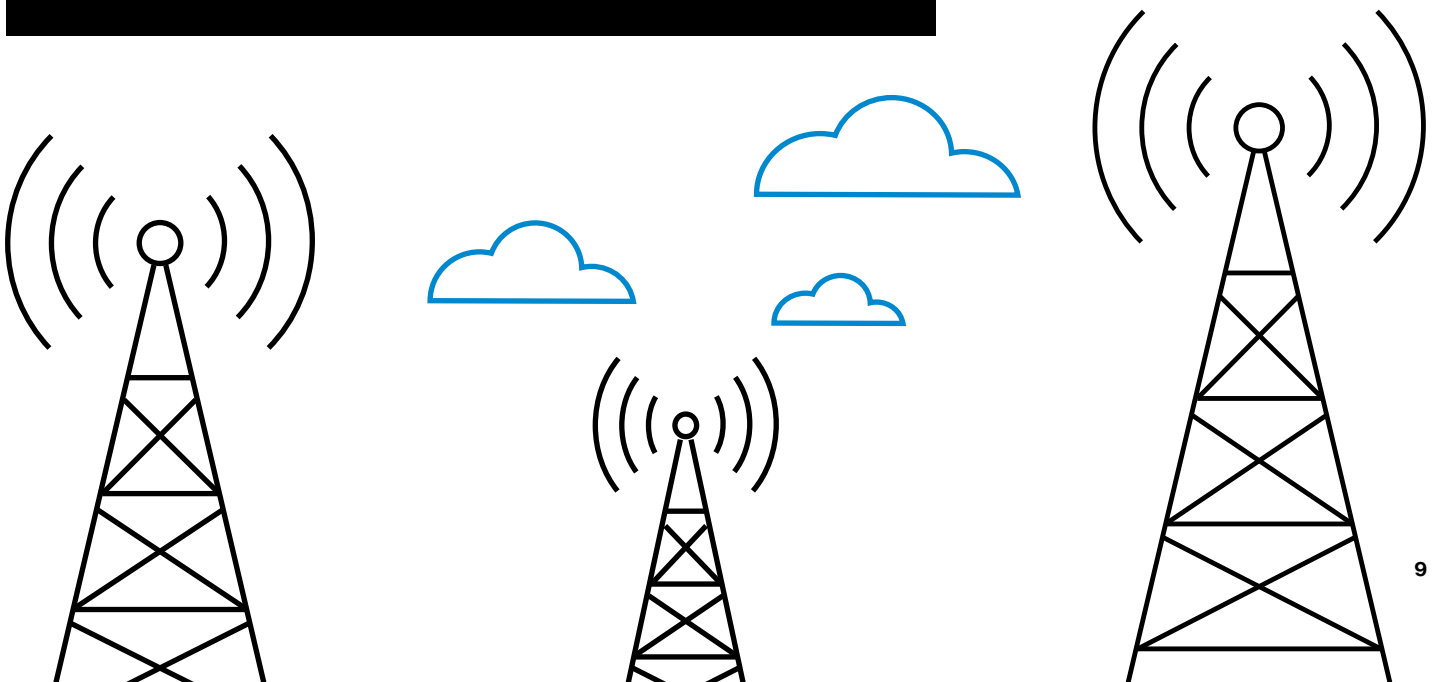
MSI 2020 industry-specific reports

Get detailed information on the state of mobile security and risks in your industry. Reports include financial services, healthcare, retail, manufacturing, the public sector and a special look at small and medium-sized businesses.

Mobile security video interview

Curious to know how we do mobile security at Verizon? This video describes our multilayered approach to mobile security as a best practice.

For more information, visit enterprise.verizon.com/msi



verizon

[1] Christopher McMahon, U.S. Secret Service
[2] Based on aggregated 2019 usage data supplied by MobileIron.
[3] Based on data from November 2018 to October 2019, Wandera Threat Research.
[4] Overall, the average mobile device connects to two to three insecure Wi-Fi hotspots per day. The most common settings are retail, hospitality and transportation hubs, including airports, as per NetMotion.