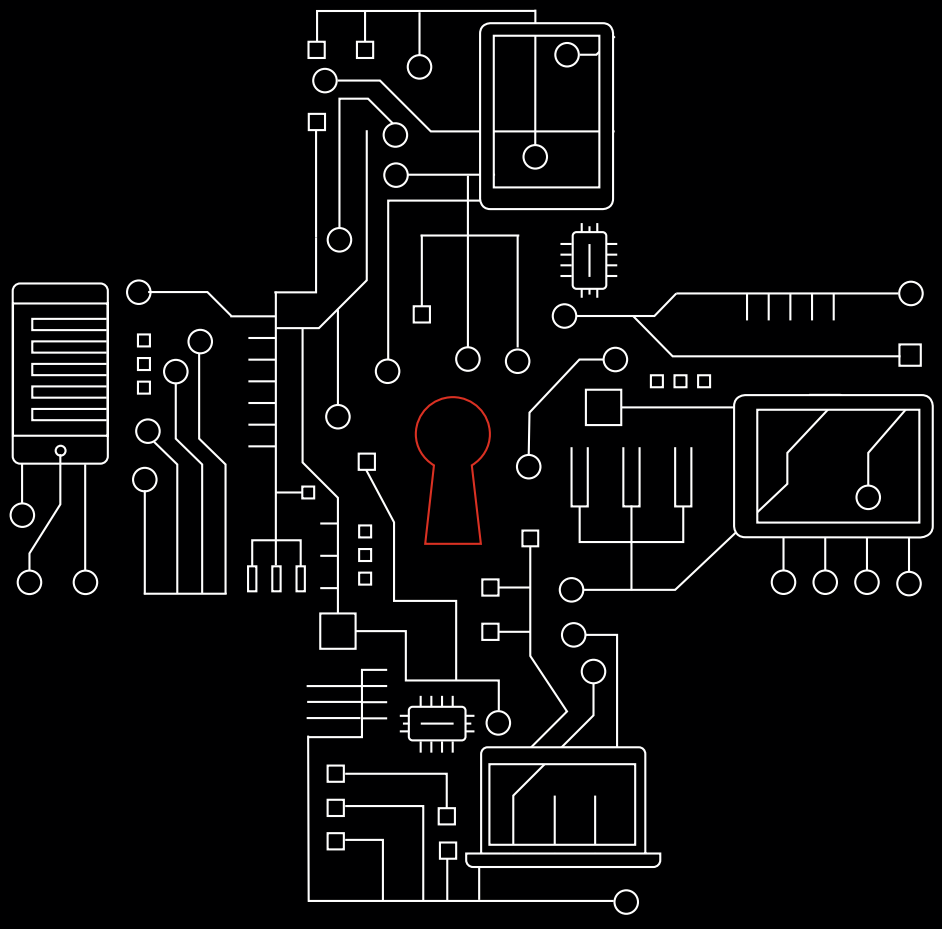
Mobile Security Index 2020

Healthcare spotlight

A deep dive into mobile security in medical centers, hospitals, ambulance services, and nursing and residential care facilities



verizon

Are you taking good care of your mobile devices?

Healthcare organizations have a lot to gain from mobile technology—but they also hold large amounts of sensitive patient data, which makes them a lucrative target for cybercriminals. Unless providers take steps to strengthen their mobile security, their data and critical systems could be at risk.

88%

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

Mobile is a potentially lifesaving tool for healthcare providers. It's helping employees to share and access medical data quickly. It's enabling better monitoring of outpatients so that staff can administer effective follow-up care and reduce readmission rates. And it's providing data-driven insights that can improve the accuracy of diagnostics and treatments. And the impact of mobile is even greater when combined with cloud-based services. Eighty-eight percent of healthcare organizations said their reliance on data stored in the cloud is growing.

We contracted an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices. In total, 876 people responded—9% of whom were from healthcare organizations, including hospitals, medical centers, ambulance services, and nursing and residential care facilities. Unless stated otherwise, all data in this report is from this survey.

verizon

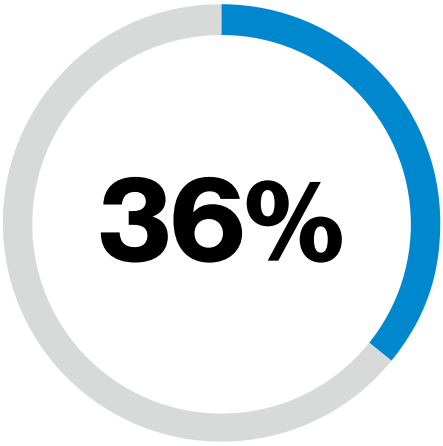
Almost two-fifths were hit.

Nearly two-fifths (38%) of healthcare organizations admitted to having suffered a compromise involving a mobile device in the past year. That's a significant rise from the previous year, when 25% of healthcare providers were compromised.

There's a lot at stake. Healthcare organizations hold highly sensitive data about their patients and employees, which can be a target for cybercriminals hoping to sell this information on the black market or conduct blackmail and extortion schemes.

In 2017, the U.K.'s National Health Service (NHS) suffered a ransomware attack that led to disruption at hospitals across the country. Thousands of patient appointments and operations had to be cancelled or transferred to other clinics.[1] And the impact of security breaches can be far-reaching. In 2019, a U.S. medical debt collector suffered a major data breach that impacted over 20 healthcare companies, including clinics and diagnostics labs. In total, almost 25 million people were affected.[2]

Despite the potential harm to patients and employees, 37% of healthcare organizations admitted they had sacrificed mobile security to "get the job done." As in other sectors, this was shown to have consequences. Healthcare organizations that said they'd sacrificed mobile security were 1.9 times as likely to have suffered a compromise.



Thirty-six percent of healthcare respondents that experienced a mobile-related compromise said that the effects were major.

37%

Thirty-seven percent of healthcare organizations said they had sacrificed security.

38%

Thirty-eight percent of healthcare organizations admitted to having suffered a security compromise.

Figure 1. Has your healthcare organization experienced a security compromise involving mobile or Internet of Things (IoT) devices during the past year? Has your healthcare organization ever sacrificed the security of mobile devices (including IoT devices) to "get the job done"?

71%

Seventy-one percent of healthcare organizations have reassessed the risks associated with mobile devices in the light of new regulations.

1,300

According to Netskope, enterprises use an average of almost 1,300 apps and cloud services, 95% of which are unmanaged, with no IT administration rights or even visibility.[3]

Healthcare organizations' biggest mobile security concerns

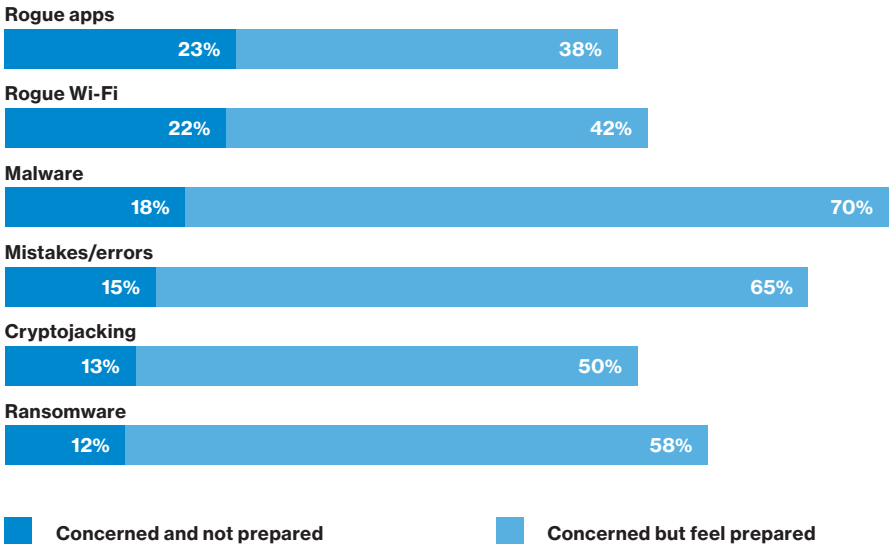


Figure 2. Please indicate how you feel about the following threats/vulnerabilities.

The risks of the cloud

Mobile and the cloud are becoming more intertwined. In fact, 85% of healthcare organizations said that within five years, mobile will be their primary means of accessing cloud-based services. For most, the cloud is now the default choice for building and running apps. Forty-four percent said that over half of their new business information is stored in the cloud.

Most healthcare respondents massively underestimate the number of apps being used in their organization. Sixty-five percent said the number was under 100. Just 4% said that they use over 1,000. The average is actually much higher.

Fear of the known

Healthcare respondents are concerned about mobile device threats—73% of respondents rated the risk to their organization as moderate to significant. They were worried about a diverse range of threats, including emerging ones like "cryptojacking." But it was well-known threats, including unapproved applications (23%), rogue or insecure Wi-Fi hotspots (22%), and malware (18%) that the most healthcare organizations felt unprepared to handle.

Healthcare providers were worried about a range of potential security breach consequences, including reputation damage (50%) and regulatory penalties (32%). But their biggest concern was suffering a loss of data (62%) and, in particular, the theft or exposure of medical records. It's not just patient information that's at risk—51% were afraid of exposing employee data, which can be a prime target for cybercriminals running highly targeted phishing scams, including tax scams.

No malice required

Medical records will always be a lucrative target for cybercriminals. But "insider threats" remain one of the biggest concerns for the sector. Seventy-five percent of healthcare organizations said they believed their employees are the greatest risk when it comes to mobile devices. Despite this, only 52% said they gave their employees ongoing training on IT security.

It's true that employee actions, even if inadvertent, can expose healthcare providers to greater risk. These range from installing unapproved apps to connecting to insecure public Wi-Fi hotspots. But with so many healthcare organizations knowingly sacrificing security, and with those responsible for setting mobile policies breaking the rules themselves, is it fair, or good risk management, to expect better from employees?

Healthcare providers could be doing more.

Despite everything that's at risk, many healthcare organizations are failing to take basic precautions. Less than half (43%) said they changed all default or vendor-supplied passwords or encrypted sensitive data when sending it across public networks. These are two of the most fundamental security measures, along with regular security testing and restricting access to data on a need-to-know basis. Only 12% had all four of these basic precautions in place.

And despite growing use of the cloud, just 35% of healthcare organizations said they restricted the use of cloud apps without a proven security rating. And only 49% said they restricted the functionality of apps when accessed from unknown networks or locations. Failing to take these precautions could put their data, patients and employees at risk.

Why are they cutting corners?

The top reasons respondents gave for sacrificing security were expediency (64%) and convenience (46%). This suggests that decision makers are concerned about the impact that security measures can have on productivity and efficiency. These are valid concerns in a medical setting, where the ability to access data and make fast decisions can be critical.

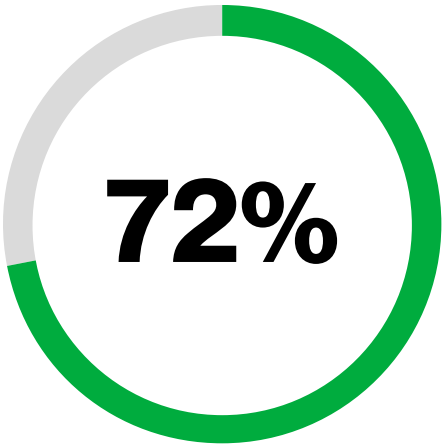
Poorly designed or implemented security policies can be bad for both employees and patients. Something as simple as a password policy could impede employees' productivity, increase support costs (due to more resets) and potentially increase risk (by driving employees to circumvent the rules, especially in medical emergencies).

Security shouldn't be a burden.

On the other hand, well-implemented security solutions can dramatically reduce risk while remaining largely transparent to users. For example, secure mobile gateways, adaptive authentication and zero-trust services can actually reduce the number of intrusive login prompts without putting systems and data at greater risk.

65%

Sixty-five percent of healthcare respondents said they personally used public Wi-Fi for work tasks, even though it was explicitly prohibited by company policy for 23% of them.



Seventy-two percent of healthcare organizations said that the need for employees to be able to access data quickly makes it harder to implement effective security.

20%

According to NetMotion, 20% of mobile workers list a restrictive IT security policy as their most frustrating issue at work—"cumbersome authentication" came fifth overall.[4]

Healthcare IoT: Increase of threat?

The volume and variety of devices using wireless connectivity has grown massively. Smart IoT devices are transforming medical services. The majority (94%) of healthcare respondents said that IoT devices are crucial to digital transformation.

Innovations like pills in smart packaging are helping to improve patient adherence to medication, while sensors in ambulances can transmit the diagnostics of patients en route to the hospital. Specifically, healthcare respondents said they're using IoT to monitor equipment and efficiency (77%), the physical security of buildings (71%), and the wellness or condition of patients (59%).

To investigate the risks of IoT, we interviewed an additional group of healthcare professionals responsible for the procurement, management and security of these devices. Seventy-seven percent of them said their organization is at risk from attacks targeting IoT devices, rating the threat moderate to significant. And 35% said they had already suffered a compromise involving an IoT device.

Despite their fears, 35% of healthcare respondents said they had sacrificed IoT security to "get the job done." Why are they cutting corners? Expediency: All of them said that time pressure was one of the reasons behind the decision. In the drive to innovate quickly, it seems security often takes a back seat. Twenty-seven percent said that IoT device security isn't a priority for version 1.0; it's something they can "worry about later."

Securing your IoT devices

Fortunately, there's a lot that can be done to improve IoT security. As well as following our recommendations for all mobile devices, implementing these four IoT-specific best practices could help you protect your organization:

1. Review security before you buy anything.
Whether you are buying off-the-shelf solutions or components to build your own IoT devices, ask potential vendors to supply details of the security measures they take, and review them for robustness. Pay particular attention to their authentication, encryption and patching policies. Seventy-six percent of respondents said they had IoT devices in remote or difficult-to-access locations. Use over-the-air (OTA) updates to help keep these devices secure.

2. Harden all devices before attaching them to your network.
First make sure that the device itself is tamper-resistant and tamper-evident. Then make sure that you change all default or vendor-supplied passwords. Also, reduce exposure by shutting down anything you don't need—if you're not using a port or protocol, block it.

3. Encrypt data in transit and at rest.
Eighty-three percent of respondents said that they are collecting personally identifiable information (PII), and 25% of those weren't encrypting it. Encrypting data can make it useless to hackers and help you mitigate the risk of a reputation-destroying data breach.

4. Use an IoT platform.
Choose an IoT platform that enables you to monitor and manage all your devices easily. This can help you reduce vulnerabilities by implementing digital certificates and other security features. An IoT platform can also help mitigate attacks by limiting the potential damage of SIM theft by binding SIMs to devices.

44%

Forty-four percent of the companies that made products with IoT built in used digital certificates to improve security.

93%

Ninety-three percent of healthcare respondents said they think organizations need to take mobile device security more seriously.

71%

Seventy-one percent of healthcare organizations said they think the risk associated with IoT devices has increased in the past year.

Don't wait until you get bitten.

Ninety-three percent of healthcare respondents said they believed that organizations need to take mobile device security more seriously. And 77% said they think that mobile device threats were growing more quickly than others.

Thirty percent of healthcare organizations that had experienced a compromise said that their mobile security spend had increased significantly in the past year compared to just 16% for those that hadn't suffered a breach.

While it's good to see that healthcare providers recognize the problem, it's worrying that they're not taking more concrete steps to protect themselves.

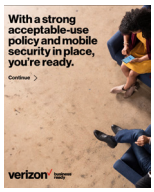
The consequences of a mobile-related security incident are often serious and far reaching. Of healthcare respondents that had suffered a compromise, almost half (48%) experienced downtime as a result of the attack, and 39% had to deal with the loss or exposure of data. Remediation can be lengthy, difficult and expensive.

Don't wait until you discover a breach to rethink your mobile security. It's time to act.

Next steps

MSI 2020 main report
This spotlight is an offshoot of the full Mobile Security Index (MSI) 2020 report. The extended report provides 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
This online assessment tool uses insight from the MSI report to rate your organization's mobile security maturity in four key areas: understanding, perception of risk, exposure and preparedness. Use it to identify where to focus to improve your security posture.



MSI 2020 acceptable use policy guide
This 10-step guide can help you build a comprehensive acceptable use policy (AUP) that helps your employees understand what is, and isn't, acceptable when using mobile devices. This can help mitigate the risk of threats like malware and phishing.

Recommendations

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 solution to simplify patch management and enforce your AUP, including authentication policies
- Deploy mobile threat detection software to regularly scan 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 that use trusted networks or VPNs

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

About Verizon Mobile Security Index

Now in its third edition, the MSI is a leading source of information on mobile security. This year, we commissioned an independent survey of 876 professionals responsible for buying, managing and securing mobile and IoT devices for their organization. To add further insight, we worked with Asavie, IBM, Lookout, MobileIron, NetMotion, Netskope, Symantec, VMware and Wandera, all leaders in mobile device security. They provided additional information, including incident and usage data. We also worked with the FBI and the U.S. Secret Service. We'd like to thank all of our contributors for their valuable contributions in helping us present a more complete picture of the threats impacting mobile devices and what is being done to mitigate them.

verizon

1 "NHS 'could have prevented' WannaCry ransomware attack," BBC, October 27, 2017.
2 "AMCA Data Breach Total Nears 25M as Wisconsin Diagnostic Laboratories Confirms 115K Record Breach," HIPAA Journal, August 28, 2019.
3 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019
4 Employee Frustration Index, a survey of 285 individuals covering a wide range of age groups and device types across North America, NetMotion, September 2019, https://www.netmotionsoftware.com/blog/connectivity/mobile-frustration-index