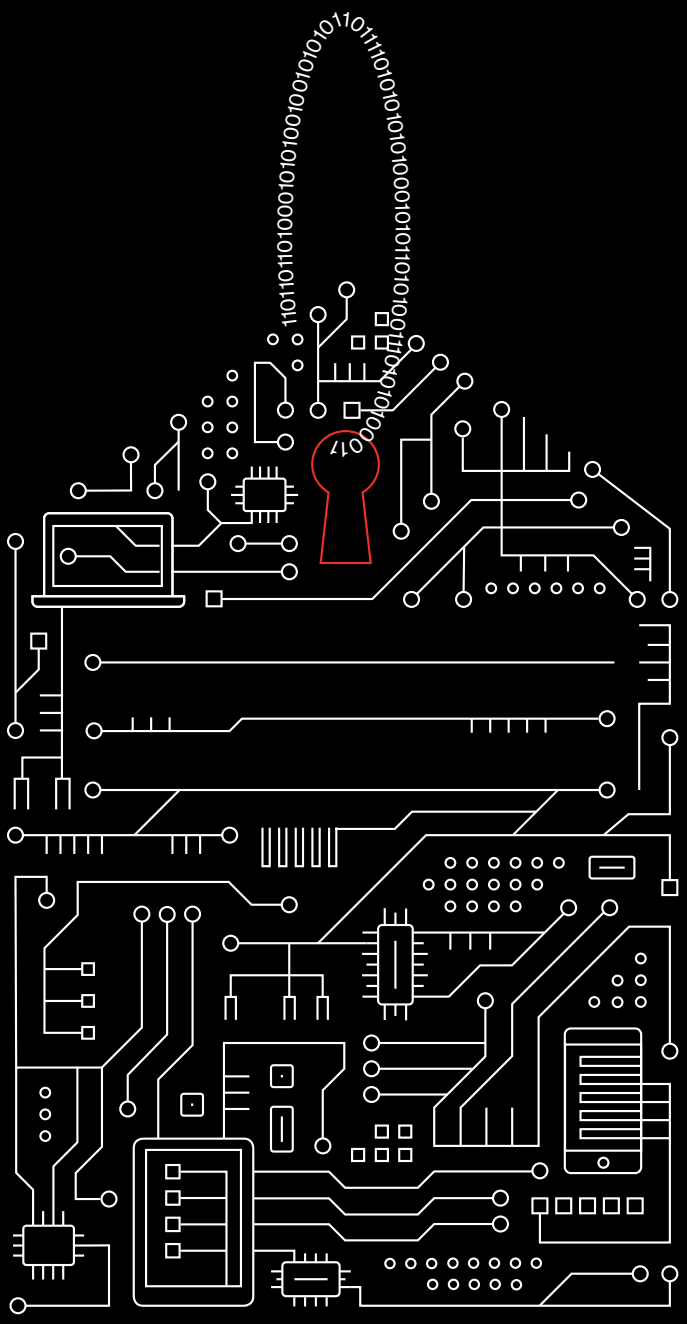
Mobile Security Index 2020

Retail spotlight

A deep dive into mobile security in the retail, travel and hospitality industries



verizon

Are your mobile devices putting your customers' data and loyalty at risk?

Cybersecurity is no longer a topic just for IT. Privacy and data protection are often in the news and regularly discussed in the boardrooms of retail, travel and hospitality companies.

83%

Eighty-three percent of retailers said that mobile devices are critical to the smooth running of their organization.

The power and versatility of mobile devices are helping retailers appeal to the modern consumer and keep physical stores relevant. Combined with cloud-based services, they're giving some companies the edge to compete and win – especially smaller businesses, 83% of which said the cloud is helping them level the playing field against larger enterprises.

But as they continue to leverage mobile technology to deliver better customer experiences and greater efficiency, many retailers could be doing more to keep their data safe.

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—over 8% of whom were from retail organizations. This includes retail, travel and hospitality companies of all sizes. Unless stated otherwise, all data in this report is from this survey.

verizon

Almost one in three were hit.

Nearly a third (30%) of companies in the retail, travel and hospitality industries admitted to having suffered a compromise involving a mobile device in the past year. That's almost unchanged from our previous report, despite the abundance of news items about companies that suffered a breach and the corresponding damage to their results and reputations.

Big and small, niche to household name—retail companies of all sizes have suffered. The parent company of a U.S. restaurant chain was hit with a malware-based attack, and the details of 2 million payment cards were exposed.[1] One of Europe's biggest airlines suffered a breach that led to the details of 500,000 customers being harvested.[2] And our research found that 28% of small and medium-sized businesses (SMBs) suffered security breaches that involved a mobile device.

87%

Eighty-seven percent of retailers said that a mobile security compromise could have a lasting impact on customers' loyalty to their brand.

40%

Forty percent of retailers said they had sacrificed security.

30%

Thirty percent of retailers admitted to having suffered a security compromise.

Figure 1. Has your retail, travel or hospitality company experienced a security compromise involving mobile or Internet of Things (IoT) devices during the past year? Has your retail, travel or hospitality company sacrificed the security of mobile devices (including IoT devices) to "get the job done"?

Despite the potential damage to customer loyalty and brand value, 40% of retailers admitted they had sacrificed security to "get the job done." As in other sectors, this was shown to have consequences. Retailers that said they'd sacrificed security were 1.5 times as likely to have suffered a breach.

Mobile is transforming retail.

There's no disputing the importance of mobile. It's helping retailers transform the customer experience by combining online services with the tactile experiences offered by brick-and-mortar stores. It's enabling greater convenience for shoppers through innovations like self-service kiosks and mobile point of sale. It's empowering employees to serve their customers better. And it's streamlining inventory management while helping to control costs and cut waste from the supply chain.

Many of the things that retail, travel and hospitality companies are using mobile devices for are enabled by the cloud. For most, it's now the default choice for building and running apps. Sixty-two percent said that over half the new business information they create is stored in the cloud.

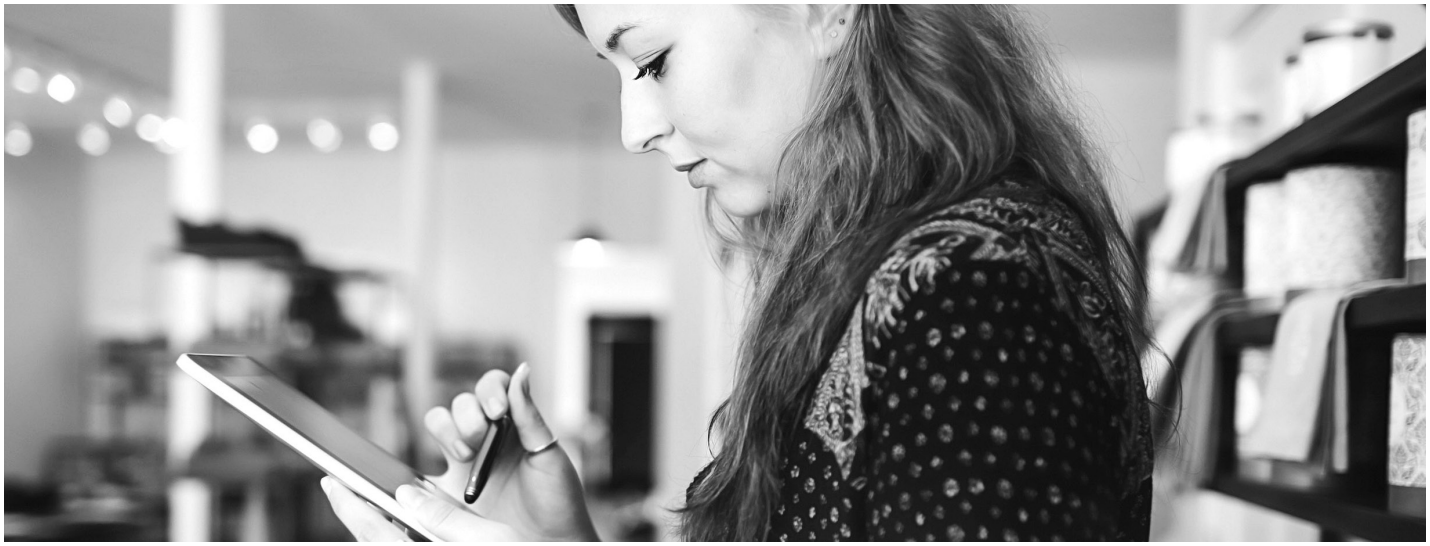
Most retailers massively underestimated the number of apps being used in their organization. Half said the number was under 100. Just 11% said that they use over 1,000. The average is actually much higher.

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]

80%

Eighty percent of our respondents said that within five years, mobile will be their primary means of accessing cloud services.



33%

A third (33%) of retail respondents said they have seen rogue hotspots using their brand name. Attackers can use these hotspots to spy on users' browsing, intercept credentials and even push malicious malware to unsuspecting customers' devices.

Retailers' biggest mobile security concerns

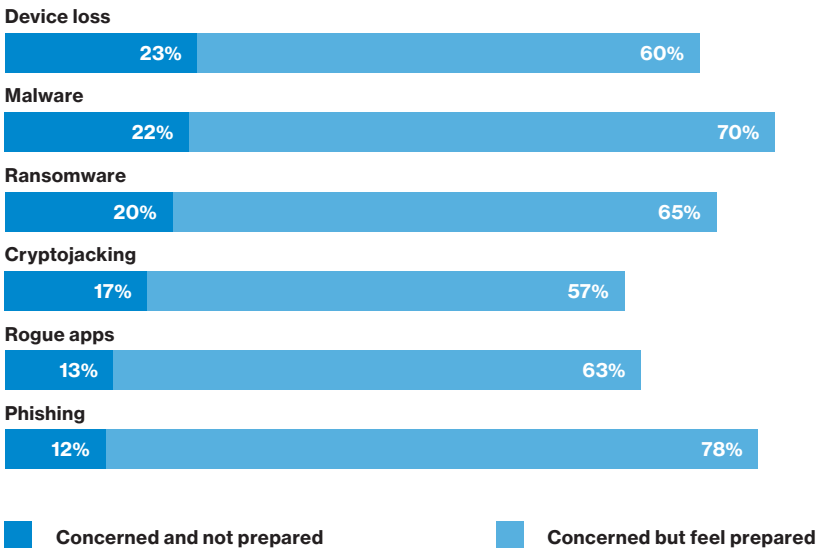


Figure 2. Please indicate how you feel about the following threats/vulnerabilities.

Fear of the known

Retailers are concerned about mobile device threats—77% rated the risk to their business as moderate to significant. They said they were worried about a wide range of threats, including emerging ones like "cryptojacking." But it was most common for retailers to feel unprepared for well-known ones—like device loss or theft (23%), malware (22%) and ransomware (20%)—than newcomers.

While retailers said they were concerned about downtime and delays to their supply chains, more (71%) said that they were worried about the theft of customer data. And an even greater proportion (74%) said they were concerned about staff records being compromised. Employee data is a prime target for cybercriminals running highly targeted phishing schemes, including tax scams.

No malice required

In recent years, “insider threats” have received much attention. And 78% of retailers said they think their employees are the greatest risk when it comes to mobile devices.

It’s true that employee actions, even if inadvertent, can expose companies to greater risk. These range from installing unapproved apps to connecting to insecure public Wi-Fi hotspots. And this problem is often exacerbated by having part-time and seasonal staff. But with so many companies 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?

While 88% of retailers said their frontline staff use mobile devices, only 37% said that these employees have a high level of cybersecurity awareness. And only 45% said that they gave staff ongoing training on cybersecurity.

Retailers could be doing more.

Despite the high stakes, many retailers are failing to take basic precautions. Less than half (47%) said they changed all default or vendor-supplied passwords. And only 43% said they 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 17% of retailers had all four of these basic precautions in place.

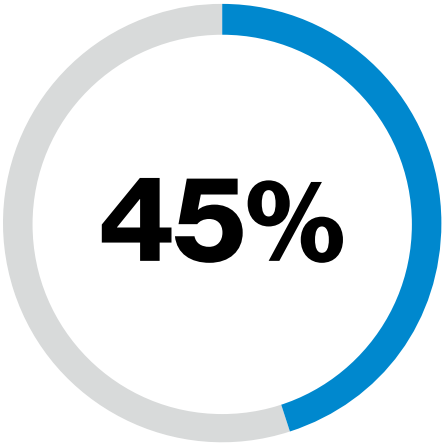
And despite growing use of the cloud, 18% of retailers said they didn’t take any special measures to secure their cloud-based services. Just 40% said they restricted the use of cloud apps without a proven security rating. And only about half said they blocked the use or restricted the functionality (51%) of cloud apps when accessed from unknown networks or locations. Failing to take basic precautions like these can put customer, employee and business data at greater risk.

Why are retailers failing to act?

The top three reasons respondents gave for sacrificing security were pressure to meet profitability targets (54%), convenience (54%) and expediency (46%). This suggests that as well as budget considerations holding companies back, decision makers are concerned about the impact that security measures can have on productivity and efficiency. Badly designed or implemented security policies can hurt the employee experience and company performance. 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).

70%

Seventy percent of retail respondents said that they personally used public Wi-Fi for work tasks, even though it was explicitly prohibited by company policy for 31% of them.



Nearly half (45%) of retailers said that lack of budget was hindering their efforts to improve mobile device security.

Retail IoT: Increase of threat?

The volume and variety of devices using wireless connectivity has grown massively. Smart IoT devices are transforming the retail, travel and hospitality sectors. Sixty-seven percent of respondents from these industries said that IoT devices are crucial to digital transformation.

Retailers are using IoT devices to enhance the customer experience with features like digital signage (67%), improved physical security of their buildings (67%), and increased equipment utilization and employee productivity (60%).

To investigate the specific risks of IoT, we interviewed an additional group of retail sector professionals responsible for the procurement, management and security of these devices. Eighty-seven percent of them said their business is at risk from attacks targeting IoT devices, rating the threat moderate to significant. And 47% said they had already suffered a compromise involving an IoT device – over 50% more than said the same about other mobile devices.

Despite their fears, 33% said they had sacrificed IoT security to "get the job done." Why are they cutting corners? Expediency: 80% said that time pressure was behind the decision. To survive, retailers need to offer innovative customer experiences that are as good as or better than what their competitors are doing. But in the drive to get to market quickly, 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.

47%

Forty-seven percent of retailers said they thought the risk associated with IoT devices has increased in the past year.

78%

Seventy-eight percent of retailers expect new vulnerabilities to increase the risk associated with IoT devices.

67%

Sixty-seven percent of retailers that were using IoT had at least one full-scale deployment.

Don't wait until you get bitten.

Sixty-one percent of retailers that had experienced a compromise said that their mobile security spend had increased significantly in the past year, and 56% said they expected it to increase significantly in the coming year. The corresponding numbers for those that hadn't suffered a compromise were just 19% and 17%.

90%

Ninety percent of retailers said they think that organizations need to take mobile device security more seriously.

While it's good to see that companies are taking steps to rectify mobile security issues, it's worrying that so many seem to wait until they personally suffer a compromise.

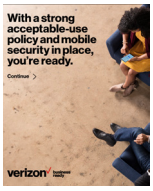
The consequences of a mobile-related security attack can be serious and the repercussions lasting. Sixty-one percent of retailers that suffered a compromise said remediation was difficult and expensive.

Don't wait until you discover a breach to rethink your mobile security. Now is the 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 the 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 "The biggest security breaches of 2019, so far," Komando.com, August 8, 2019.
2 "British Airways faces record £183m fine for data breach," BBC, July 8, 2019.
3 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019