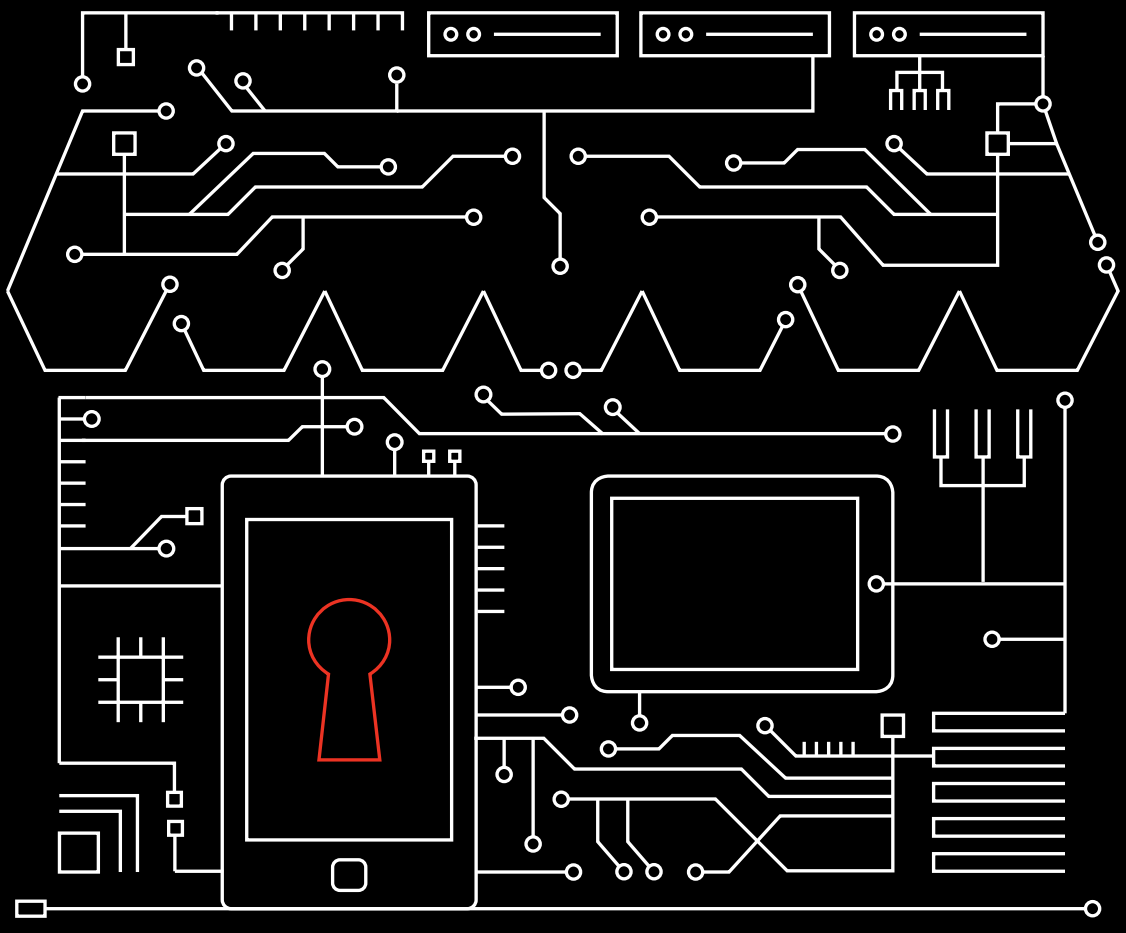
Mobile Security Index 2020

SMB spotlight

A deep dive into mobile security in small and medium-sized businesses



verizon

Could poor mobile security put a big dent in your small business?

Mobile technology and the cloud are enabling small and medium-sized businesses (SMBs) to grow and compete with larger enterprises more effectively. But unless they take further steps to secure their mobile devices, SMBs could face significant damage to their reputation and bottom line before the competition even begins.

SMBs might lack the resources and IT budgets of larger enterprises, but it's not holding them back when it comes to innovation. In many cases, SMBs are quicker to adopt new ways of working. With the business productivity apps available today, SMBs are able to give employees more powerful and user-friendly tools that belie their size. This explains why 80% of SMBs said that accessing business systems on mobile devices is key to their profitability and productivity. And it's an even bigger game-changer when combined with the cloud. Eighty-three percent of SMBs said that cloud-based services are helping them to grow and compete with larger businesses.

80%

Eighty percent of SMBs said that accessing business systems on mobile devices is key to their profitability and productivity.

39%

Thirty-nine percent of SMBs believed they're more of a target for cybercriminals than larger enterprises.

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 30% of whom were from small to medium-sized businesses. Unless stated otherwise, all data in this report is from this survey.

verizon

More than one in four were hit.

Twenty-eight percent of small businesses admitted to having suffered a compromise involving a mobile device in the past year. This number shows almost no year-over-year improvement with the findings in the 2019 Mobile Security Index.

That's cautionary, given the major impact that data breaches can have on smaller businesses. Smaller companies often lack the in-house expertise to react quickly and mitigate the damage a compromise can cause. These businesses can be crippled by the fines imposed in the wake of a breach, or by the harm to their reputation. According to the National Cyber Security Alliance, 25% of SMBs hit with a cyberattack in 2019 were forced to file for bankruptcy.[1] A further 10% had to be shut down completely.[2]

Despite the potential for a data breach to destroy everything they've worked toward, 39% of SMBs admitted they had sacrificed mobile security to "get the job done." As with bigger companies, this was shown to have serious consequences. SMBs that sacrificed mobile security were nearly twice as likely to have suffered a compromise.

Mobile is leveling the playing field.

Sophisticated technology is no longer the sole province of large enterprises. Affordable mobile services and cloud apps are enabling SMBs to provide remote access to crucial business information and systems. This is empowering employees to work from almost anywhere, driving efficiency and putting sophisticated data-driven insights into the hands of SMB owners.

Many of the processes SMBs are using are executed on mobile devices and powered by the cloud. In fact, 75% of SMBs said that within five years, mobile will be their primary means of accessing cloud-based services. For most, cloud-based mobile apps are now the default choice. Forty-nine percent said that over half of the new business information they create is stored in the cloud.

55%

Fifty-five percent of SMBs believed that compared to larger enterprises, they have more to lose from a security compromise.

76%

Seventy-six percent of SMBs said that mobile devices are critical to their organization.

75%

Seventy-five percent of SMBs said that within five years, mobile will be their primary means of access to cloud-based services.

39%

Thirty-nine percent of SMBs said they had sacrificed security.

28%

Twenty-eight percent of SMBs admitted to having suffered a security compromise.

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

81%

Eighty-one percent of SMBs said that the risk to their business was moderate to significant.

69%

Sixty-nine percent of SMBs said they were worried about the theft of customer data.

66%

Sixty-six percent of SMB respondents said they personally used public Wi-Fi for work tasks, even though 25% said it was explicitly prohibited by company policy.

30%

Only 30% were using an external vendor to manage their smartphone security.

Fear of misuse and abuse

While they are seizing the advantages that cloud and mobile offer, SMBs are increasingly concerned about mobile security threats. Eighty-one percent said that the risk to their business was moderate to significant. They were worried about a wide range of threats, from well-known attack methods like phishing, malware and ransomware, to emerging ones like "cryptojacking." But it was most common for SMBs to feel unprepared for threats that they are exposed to through employee behavior—like using devices to access adult, gambling or illegal content (21%) or the use of unapproved or rogue applications (20%).

While 38% of SMBs said they were concerned about the exposure of their intellectual property, more (69%) said they were worried about the theft of customer data. A similar proportion (67%) said they were concerned about staff records being compromised. Employee and customer data is a prime target for cybercriminals running highly targeted phishing schemes, including tax scams.

Agility isn't a panacea.

Many SMBs think their agility gives them an advantage when it comes to cybersecurity. Fifty-two percent said that SMBs can react more quickly than larger enterprises, making it easier to respond to attacks. But speed isn't enough if you don't have the right resources at your disposal. SMBs often don't have dedicated mobile security teams in-house. And despite the gaps in their expertise, only 30% were using an external vendor to manage their smartphone security.

And SMBs are knowingly failing to protect themselves against "insider threats." Seventy-two percent said their employees are the greatest risk when it comes to mobile devices. Yet almost half (49%) said they don't give their employees ongoing training on IT security.

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. But with so many SMBs knowingly sacrificing mobile security and breaking their own rules, is it fair, or good risk management, to expect better from employees?

SMBs could be doing more.

Despite the high stakes, many SMBs are failing to take basic precautions. Only 50% restricted access to data on a "need to know" basis. And just 41% said they change all default or vendor-supplied passwords. These are two of the most fundamental security measures, along with regular security testing and encrypting data when sending it across public networks. Only 11% of SMBs had all four of these basic precautions in place.

And despite growing use of the cloud, SMBs were less likely than other companies to have specific measures in place to secure their cloud-based services—27% of SMBs didn't, compared to 17% of all organizations. Just 47% said they restrict the use of cloud apps that lack a proven security rating. And only 48% restricted the functionality of cloud apps when accessed from unknown networks or locations. Failing to take precautions like these can put customer, employee and business data at greater risk.

SMBs' biggest mobile security concerns

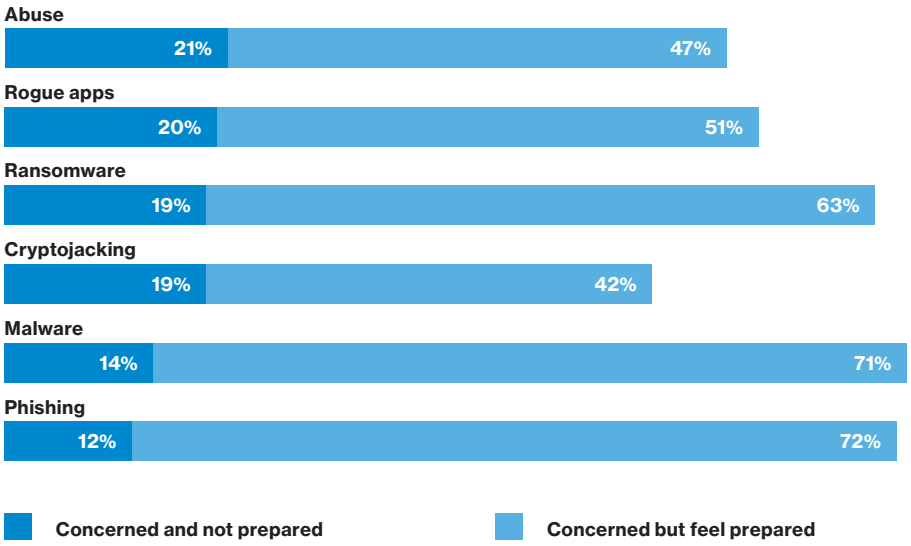


Figure 2. Please indicate how you feel about the following threats/vulnerabilities.

Sixty percent of SMBs that experienced a mobile-related compromise said that the effects were major, and 30% said that it had lasting repercussions.

Why are SMBs failing to act?

The top three reasons SMBs gave for sacrificing security were expediency (61%), pressure to meet profitability targets (45%) and convenience (42%). This suggests that SMBs are concerned about the impact that security measures can have on productivity and efficiency.

Badly designed or implemented security policies can be bad for the employee experience and company performance. If implemented poorly, something as simple as a password policy could impede employees' productivity, increase support costs (due to more resets) and potentially increase risk (by driving users to bypass the rules).

Security shouldn't be a burden.

On the other hand, well-planned and well-executed 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.

Effective tools can also help reduce the burden on IT teams, improve reporting and increase visibility.

92%

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

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.[3]

43%

Forty-three percent of SMBs that suffered a mobile security compromise said remediation was difficult and expensive.

verizon

SMB IoT: Increase of threat?

The volume and variety of devices using wireless connectivity has grown massively. Smart IoT devices are helping many SMBs to gain a competitive edge. Seventy-seven percent of respondents said that IoT devices are crucial to digital transformation.

SMBs are using IoT devices to improve efficiency and monitor equipment or productivity (56%), to monitor the physical security of buildings (54%), and to track the movement of people, vehicles or shipments (49%).

To investigate the specific risks of IoT, we interviewed an additional group of SMB professionals responsible for the procurement, management and security of these devices. Seventy-seven percent of them said that their business is at risk from attacks targeting IoT devices, rating the threat moderate to significant. And 26% said they had already suffered a compromise involving an IoT device.

Despite their fears, 38% said they had sacrificed IoT security to "get the job done." Why are they cutting corners? Expediency—53% said that time pressure was behind the decision. In the drive to innovate quickly, it seems security often takes a back seat. Over a fifth (22%) of SMB IoT users 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 organizations that made products with IoT built in used digital certificates to improve security.

88%

Eighty-eight percent of SMBs said they think organizations need to take IoT device security more seriously.

54%

Fifty-four percent of SMBs said they think the risk associated with IoT devices has increased in the past year.

77%

Seventy-seven percent of SMBs said IoT devices are crucial to digital transformation.

Don't wait until you get bitten.

Forty percent of SMBs that had experienced a compromise said they'd increased their mobile security spend significantly in the past year, and 36% said they expected it to increase significantly in the coming year. The corresponding stats for those that hadn't suffered a compromise were just 12% and 10%.

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

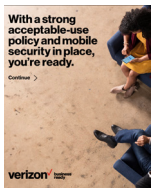
The consequences of a mobile-related security compromise can be serious and the repercussions lasting, and bouncing back can be especially hard for smaller businesses. Forty-three percent of SMBs that suffered a compromise said remediation was difficult and expensive.

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 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—nearly a third of which were from small and medium-sized businesses—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 Small Business Cyber Criminal Target Survey Data, National Cyber Security Alliance, October 2019.
2 Small Business Cyber Criminal Target Survey Data, National Cyber Security Alliance, October 2019.
3 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