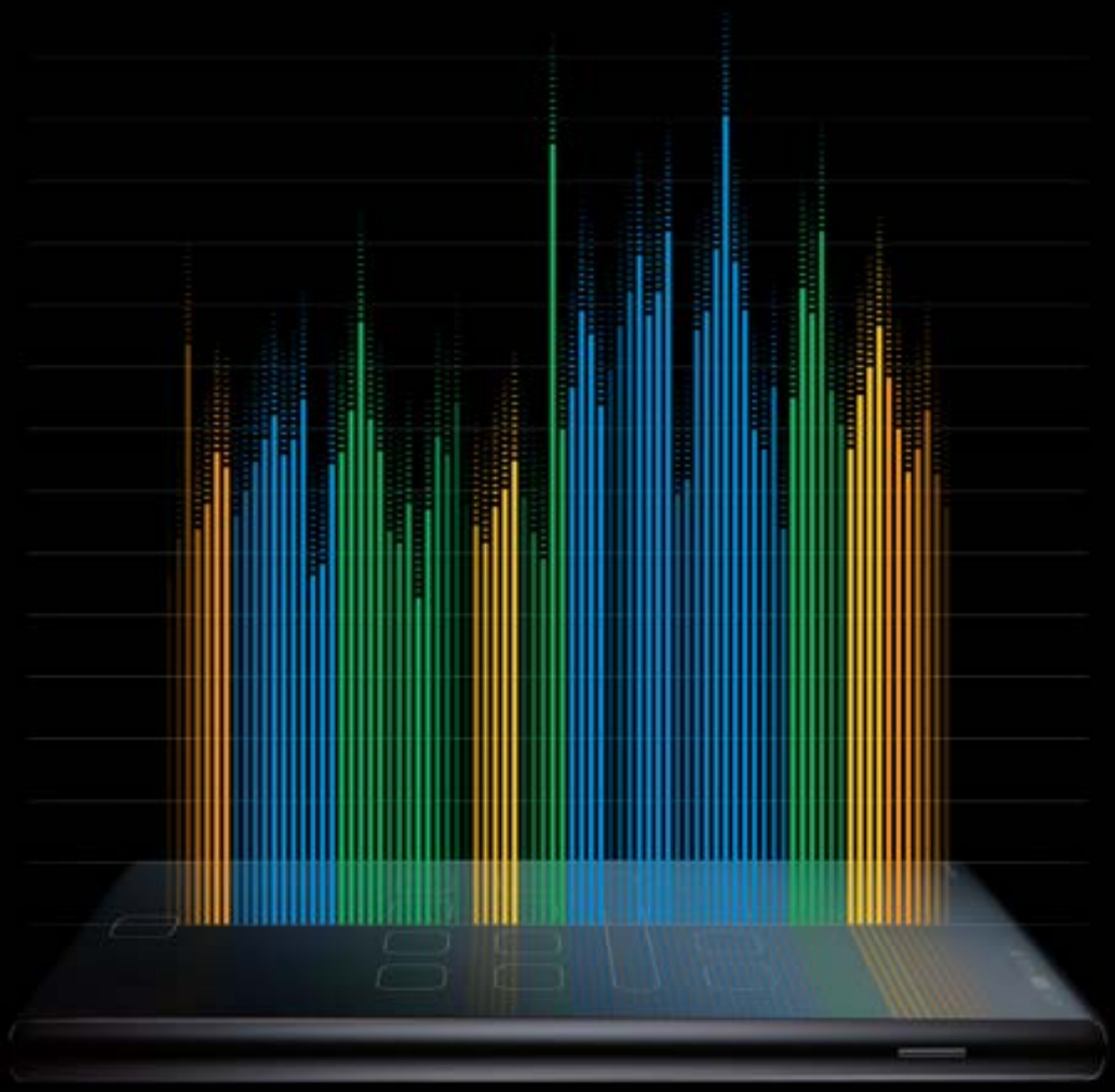
Mobile Security Index 2021

SMB spotlight

A deep dive into the state of mobile security in small and medium businesses.



verizon

Onsite or offsite, they shouldn't be out of mind.

Small and medium businesses (SMBs) may lack the resources and IT budgets of large enterprises, but mobile and cloud-based technologies are leveling the playing field.

But if a mobile security breach happens, SMBs can be crippled by the aftermath. They often lack sufficient in-house expertise to react quickly and mitigate the damage. And they can find it difficult to bounce back from the financial losses. Almost two-thirds (65%) of SMBs that responded to the Mobile Security Index (MSI) survey said that they have more to lose from a security breach than larger enterprises.

In this report, we explore some of the specific challenges facing SMBs and how the increase in working from home has affected their security readiness. Unless otherwise stated, data in this report is based on the responses of SMB participants—those working at companies with fewer than 500 employees—in the latest MSI survey.

65%

Nearly two-thirds of SMB respondents said that cloud-based services are helping them to compete with larger companies.

52%

Over half of SMB respondents to the MSI survey said that they think they are more of a target than larger enterprises.



Mobile is helping to level the playing field.

Powerful mobile devices and cloud apps are enabling SMBs to help employees be productive from virtually anywhere. This helps to explain why many SMBs now have a mobile-first and cloud-first strategy. In our survey, almost half (47%) of SMB respondents said that the shift had reached the point where most of their company's data processing is now done in the cloud.

In the future, organizations will be more reliant on networks they don't own —such as cellular, public Wi-Fi and home broadband—than ones they do. Almost three-quarters (74%) of SMB respondents expect this to be the case.

SMBs were less able to adapt to COVID-19 lockdowns.

Prior to restrictions being imposed to deal with the coronavirus pandemic, According to our survey, SMBs had a slight lead over enterprises in the percentage of employees working from home at least some of the time—35% to 31%.

When lockdowns were put into force, that figure leapt 22 percentage points (pp) among the SMBs and a massive 35 pp (up to 63%) in the large enterprises represented by our respondents.

When asked why their organization had been unable to allow more people to work from home, over a third (35%) of SMB respondents said "technical issues prevented access to systems" and a quarter (25%) said "security concerns."

Both groups said that they expected the share of those working from home to fall back when all restrictions are lifted. But both predicted that it will settle at a much higher level than before. SMB respondents expected it to settle at 47%, enterprise respondents expected it to settle slightly higher at 50%.

Big enough to hide

You might think that it's only big corporations that have to worry about what's going on in the farthest reaches of the organization. But our survey suggests otherwise. Most (85%) SMB respondents said that they were concerned about shadow IT—devices, software and services outside the ownership or control of the IT organization.[1] Over a third (35%) said that they were quite or very worried. Maybe that's a downside of the "just do it" attitude that makes SMBs so nimble. But decisions being made without the oversight of IT could lead to problems.

78%

Over three-quarters of SMB respondents said that organizations need to take mobile-device security more seriously.

71%

More than two-thirds of SMB respondents said that increased working from home had moved cybersecurity up their agenda.

29%

Close to one in three SMB respondents said that the compromise their company experienced was difficult and expensive to remediate.

> **Mobile devices were critical to maintaining business continuity during lockdown by enabling employees to stay productive from home. That explains the 26% increase in their use we saw in the first 100 days."**
>
> – Aaron Cockerill, Chief Strategy Officer, Lookout

Restrictions drove a massive increase in cutting corners.

In our latest survey, 77% of SMB respondents said that they faced pressure to sacrifice security to "get the job done." And 59% said that had succumbed to that pressure. That's up from 39% in the previous edition of this report.

The most common reason cited for sacrificing security was responding to the COVID-19 crisis (41%), followed by the need to hit targets (34%) and expediency (32%).

Almost a quarter (22%) of SMB respondents said that they were aware of their company having suffered a compromise involving a mobile device in the past year. The good news is that's down from 28% in our previous survey. But it means that—despite the reductions in activity and travel due to COVID-19 lockdowns—more than one in five (22%) organizations still suffered a mobile-related incident that led to downtime or the exposure of data.

The consequences were often major.

Over two-fifths (42%) of SMB respondents who said that their organization had experienced a mobile-related compromise said that the effects were major; and half of those said that the repercussions were lasting. Just one in six described the impact as minor.

Loss of data isn't the only thing to worry about.

The consequences weren't just serious, they were multiple. Many that suffered compromises saw many negative impacts. Almost a third (30%) of SMB respondents that said their organization had experienced a compromise said that as a consequence they had:

- Suffered downtime
- Incurred damage to their reputation
- Had regulatory penalties imposed

The loss of data, which topped the list of common concerns (41%) among all SMB respondents, was actually only an outcome in 20% of compromises.



verizon

SMBs' biggest concerns

The majority (88%) of SMB respondents said that they are concerned about mobile-device threats. More than two-fifths (43%) rated the risk as high or significant.

The threats causing SMBs concern

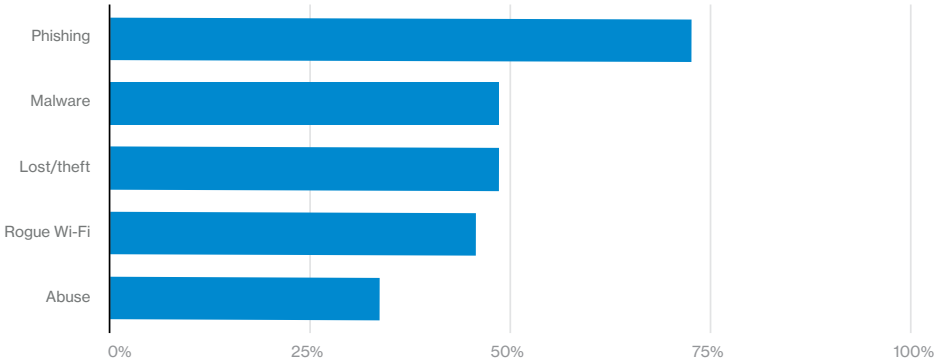


Figure 1. Please indicate which of the following threats/vulnerabilities you're concerned about—you think is a threat and feel unprepared to handle. Phishing includes variants like business email compromise, smishing and vishing.

Phishing

More SMBs were concerned about phishing than any other cybersecurity threat – and with good reason. Lookout, a mobile-security company, saw a 364% increase in the number of mobile phishing attempts in 2020 versus 2019.[2] With many employees working from home, cybercriminals have adapted their techniques to take advantage of the disruption.

Cloud-based applications can make phishing attacks more effective and facilitate business email compromise attacks, which are the leading cause of financial loss in cyberattacks. The extensive control granted to users by Microsoft 365 and similar services can give attackers in possession of stolen credentials—obtained from phishing operations—a critical foothold inside the target organization.

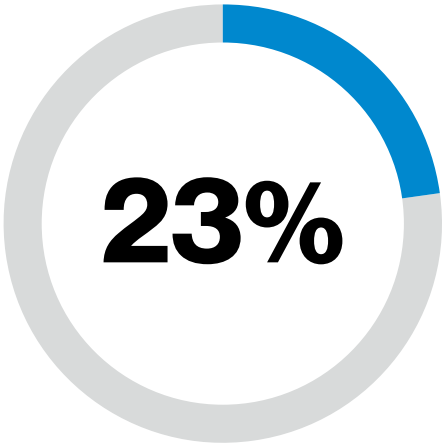
> **"We know that cybercriminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the coronavirus outbreak."**
>
> – Paul Chichester, Director of Operations, National Cyber Security Centre (NCSC)

364% ▲

Lookout saw a 364% increase in the number of mobile phishing attempts in 2020 versus 2019.[3]

26x

Mobile-device users are 26 times more likely to click on a phishing link than they are to encounter malware.[4]



Less than a quarter of respondents said their organization had a MDM or EMM solution in place.

4%

Public Wi-Fi can be dangerous, but just 1 in 25 SMB respondents said their organization blocks its use.

6x

Netskope Threat Labs saw a 600% increase in the number of visits to websites hosting adult content in the first half of 2020.[5]

Malware

Based on data from Wandera, the encounter rate for malware dropped year-over-year. In 2020, over 8% of organizations had experienced at least one malware incident—that's down from 10% in 2019, but up from 2% in 2018.[6]

Lack of employee awareness is a problem. Nearly 30% of U.S. workers said that they thought that malware is a type of hardware that boosts a Wi-Fi signal.[7] This serves as an important reminder that what might seem obvious to those working in IT and well-read on cybersecurity may be a mystery to many others. There's still a lot to do in educating employees about the threats and how to counter them—both in their personal lives and employees.

Loss/theft

People lose stuff. They leave phones, tablets and laptops in taxis, on trains, at restaurants—the list goes on and on. Some of these will end up in lost-and-found boxes, others will find a new owner—or rather a new owner will find them.

Loss/theft is one of the types of compromises that's easiest to mitigate. Protections like device encryption and remote wipe are now standard with most types of user device and mobile device management (MDM)/enterprise mobility management (EMM) solution. But that doesn't mean that people are using them.

Rogue Wi-Fi

To paraphrase a famous saying, there's no such thing as free public Wi-Fi. At best, users are swapping privacy for convenience. At worst, they could be compromising credentials to other systems and exposing devices—not just the one they're using, but everything it can connect to—to malicious code.

The dangers of public Wi-Fi are increasing as mobile devices are used for more tasks. Over two-fifths (43%) of SMB respondents that admitted that their company had suffered a mobile-related compromise said that a network threat (such as the use of public Wi-Fi) played a role in it.

Abuse

It's not just hackers that SMBs need to worry about. Misuse by employees can have numerous negative effects.

There are many gray areas when trying to define what constitutes appropriate use, especially of mobile devices. What if employees want to use their work devices to check personal emails, stream music or scroll through social media? Many people think this is a reasonable allowance in a flexible, modern workplace. This is even more true when working remotely, whether at home or on the road.

However, some behavior is clearly unacceptable, such as accessing adult, extreme or illegal content on company devices. This could increase the company's exposure to threats such as malware. Despite the risks, fewer than one in three (32%) of SMB respondents said that their organization had an acceptable use policy (AUP) in place.

It's difficult to prevent misuse if you can't define what it is. Our AUP guide could help you develop an effective policy for your organization.

IoT: Increase of threat?



The volume and variety of devices using mobile connectivity has grown massively. Smart internet of things (IoT) devices are helping many SMBs to gain a competitive edge. To investigate the risks of IoT, we surveyed an additional set of professionals responsible for the procurement, management and security of these devices.

Just short of half (49%) of these respondents said that their organization was at significant or high risk from attacks on their IoT devices. And 26% said they had already suffered a compromise involving an IoT device.

In the drive to meet targets, security often takes a back seat. Over half (55%) of the SMB respondents in our sample of IoT users said 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. In addition to 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 about the security measures they take and review them for robustness. Pay particular attention to their authentication, encryption and patching policies. Most (85%) of SMB respondents using IoT said they had 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.

Make sure that the device itself is tamper-resistant and tamper-evident. Then make sure you change all default or vendor-supplied passwords – just 28% of SMB respondents said they do this on all IoT devices. 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.

Based on the SMB respondents in our survey, most (85%) of SMBs using IoT were collecting personally identifiable information (PII) – and almost a quarter (24%) of those weren't anonymizing it. Exposure of PII can lead to sizable regulatory penalties, especially if you are found not to have taken adequate precautions – up to 4% of global revenue for those doing business in the EU or the U.K.[8] 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.

49%

Nearly half of the IoT respondents in our survey said that these devices posed a high or significant risk to their organizations.

67%

Despite their fears, over two-thirds of respondents said they had sacrificed IoT security to "get the job done." Why are they cutting corners?

- Responding to COVID-19 (43%)
- Need to meet profitability targets (40%)
- Expediency or time pressures (39%)

Top 3

According to SMB respondents, the most common purposes they were using IoT for were:

- Security (54%): Monitoring the physical security of buildings and other property, including video
- Experience (44%): Enabling services like digital signage or providing products for consumers, like wearable devices or in-vehicle services
- Efficiency (32%): Efficiency-monitoring equipment or productivity

Security shouldn't be a burden.

Poorly designed or implemented security policies can be bad for the employee experience and the performance of the company. Something as simple as a password policy could impede productivity, increase support costs (due to more resets) and potentially increase risks (by driving employees to circumvent the rules).

On the other hand, well-implemented security solutions can help to reduce risk and remain largely transparent to users. Effective tools can also help reduce the burden on IT teams, provide better reporting and increase visibility into users' adherence with policies – including those working from home.

Recommendations

Don't wait until you discover a breach to reprioritize mobile security. Some simple steps can help reduce your exposure.

Users and behaviors:

- Establish a formal AUP that specifies responsibilities for bring-your-own-device (BYOD) users, what networks can be used and what apps users can install
- Give all employees regular training and make sure they know how to report anything suspicious
- Set and communicate a password policy

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 and things:

- 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 MDM solution to simplify patch management and enforce your AUP, including authentication policies
- Deploy mobile threat detection software

Networks and cloud:

- 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
- Restrict the use of unvetted cloud apps
- Limit access to cloud services to devices that use trusted networks or virtual private networks (VPNs)

Additional content



MSI 2021 Report

This SMB Spotlight is an offshoot of the full Mobile Security Index (MSI) report. The extended report provides more detailed statistics and analysis of the threats facing mobile devices.



Self 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.



Acceptable use policy guide

This 10-step guide can help you build a comprehensive 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.

For more information, visit verizon.com/mobilesecurityindex

About the Verizon Mobile Security Index

The Mobile Security Index is a trove of detailed information on mobile device security. For the 2021 edition, the fourth, we commissioned an independent research company to survey professionals responsible for buying, managing and securing mobile and IoT devices for their organization. In total, there were 856 respondents, over a fifth (21%) from small and medium-sized businesses – defined as having fewer than 500 employees. Unless stated otherwise, all data in this report is from this survey. To add further insights, we worked with Asavie, Blackberry Cylance, Check Point, IBM, Ivanti (formerly MobileIron), Lookout, NetMotion, Netskope, Qualcomm, Proofpoint, Thales, VMware and Wandera, all leaders in mobile devices and security. They provided additional information, including incident and usage data. The FBI, the U.S. Secret Service and Europol also made valuable contributions.

verizon

1 Gartner, Glossary: Shadow IT.
2 Wandera, analysis carried out in January 2020. Data from enterprise user base.
3 Lookout, analysis of all enterprise users covering January 2019 to December 2020
4 Wandera, analysis of data from entire global customer base between January 1, 2020 and December 31, 2020
5 Netskope, analysis based on anonymized data collected from the Netskope Security Cloud platform across millions of users from January 1, 2020 through June 30, 2020.
6 Wandera, analysis carried out in January 2021. Data from enterprise user base.
7 Proofpoint, State of the Phish, August 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
8 GDPR.EU, What are GDPR fines?, February 2019

© 2021 Verizon.