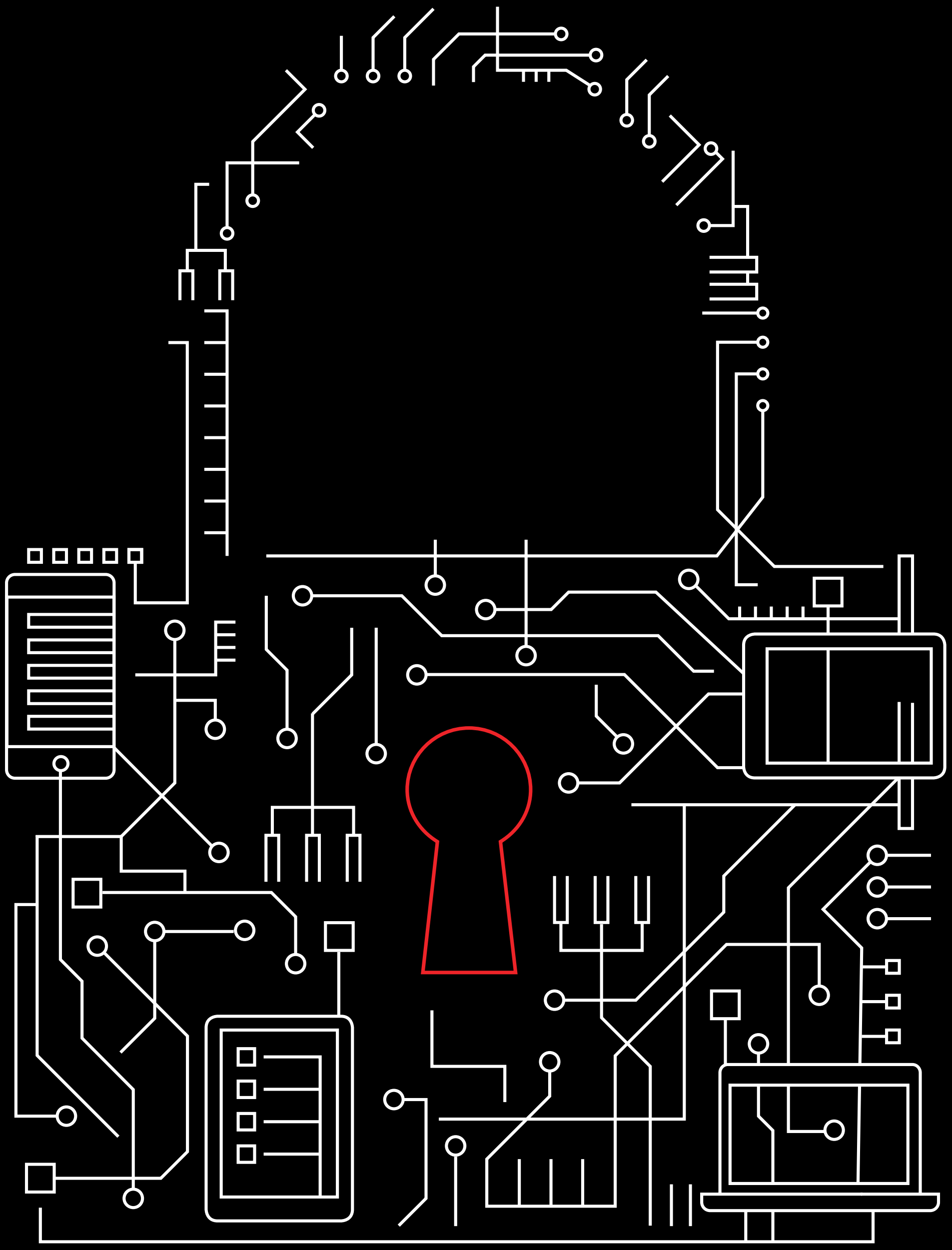
Mobile Security Index

2020 Report



verizon✓

Mobile security is the key to unlocking the potential of your cloud, internet and IoT.

Are you ready?

verizon✓

Table of contents >

Methodology

To help you assess your own mobile security environment and calibrate your defenses, we've produced this third annual Verizon Mobile Security Index. To produce it, 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. To add to this, we commissioned an independent survey of 876 professionals responsible for the buying, managing and security of mobile and Internet of Things (IoT) devices. The Federal Bureau of Investigation (FBI) and the United States Secret Service also provided valuable input. We'd like to thank all our contributors for helping us to present a more complete picture of the threats impacting mobile devices and what is being done to mitigate them.

For more information on our survey, see page 63.

Table of contents >

Foreword

The theme of this year's Mobile Security Index (MSI) is innovation. Mobile connectivity is enabling entirely new customer and employee experiences, and transforming business across all sectors. As you'd expect, we investigate 5G and the impact that that's going to have. And we look at IoT devices, most of which are connected using cellular or mobile WAN technologies, like CAT-M1 and Narrowband Internet of Things (NB-IoT).

We also look at how apps and data in the cloud are giving mobile devices increased capabilities, empowering users and becoming critical to operations. In fact, when we asked our survey respondents to rate how crucial mobile is to their business on a 10-point scale, 83% answered 8 or higher.

But that's just the beginning of the story. Unfortunately, it's not just network operators and device manufacturers that are innovating. We also explore the recurring theme of attackers getting more creative. This "mal-innovation"—from novel ways to exploit vulnerabilities to new ways to monetize attacks—is making protecting mobile devices, and all the data and resources they connect to, an ongoing challenge for business.

Mobile security is not a new issue, but the stakes are getting higher. The scale of regulatory penalties is growing, and customers—consumers, businesses and public-sector organizations—are becoming more sensitive to the issue. In the past, many people saw little difference between the approaches of the companies pursuing their business—from banks to retailers—and so it didn't sway their loyalty. That's changing, and many companies are responding by making security and data privacy central to their value proposition. We found that 84% of companies think that data privacy will be a key brand differentiator in the future.

Unfortunately, many companies only get cybersecurity right 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.

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; it's also vital to have an approach that puts mobile security right at the heart of your IT strategy.

Read on to find out more about the current mobile security environment and understand the risks. With this insight, you'll be in a better position to strengthen your mobile security as your digital transformation journey unfolds.

Table of contents ›

Terminology

Throughout this report, when we refer to companies, businesses or organizations, we include both public- and private-sector entities of all sizes. We use the term "enterprise" to refer to organizations with 500 or more employees and "small and medium-sized businesses" (SMBs) for those with fewer.

Security terms like "attack" and "breach" are often used Interchangeably. For clarity and precision, we have used the following definitions throughout this report:

Attack: A general term covering any deliberate action toward a system or data that is unauthorized. This may be as simple as attempting to access it without permission.

Compromise: A successful attack that results in a system's defenses being rendered ineffective. This could involve data loss, downtime, other systems being affected or no detrimental effects at all. It could be malicious or accidental.

Data breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

Exploit: A definition, often in the form of a script or code, of a method to successfully leverage one or more vulnerabilities to access a system without proper authorization.

Incident: This covers any form of security event, malicious or not, successful or not. This might be anything from the logging of a failed authentication attempt to a successful compromise and data breach. It also includes nonmalicious events such as the loss of a device.

Risk: A measure of the likelihood of a threat, an organization's vulnerability to said event and the scale of the potential damage.

Threat: Any danger that could impact the security of systems or privacy or data. This can apply to a technique, such as phishing, or an actor, such as organized crime.

Vulnerability: A weakness that could be exploited. It may be known or unknown—to the manufacturer, developer, owner or world.

Table of contents

This is an interactive PDF. Click on any section in this table of contents to be directed there.

Back to table of contents ›

1

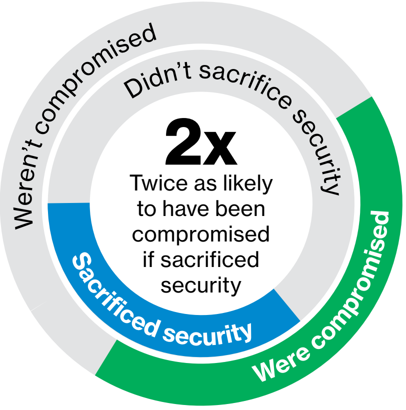
The state of mobile security

Every year, we've seen the number of companies suffering mobile security compromises rise, and this year was no exception. Despite everything that's at stake, many businesses still sacrificed security—and those that did were more likely to have been hit.

verizon✓

Are you ready?

Because more organizations are falling victim. Despite fewer cutting corners.



43%

Forty-three percent of companies sacrificed security.

39%

Thirty-nine percent of companies suffered a security compromise.

Figure 1. Intersection of organizations that have knowingly sacrificed security and those that admit to having suffered a mobile-related security compromise

The problem just keeps getting bigger.

This is the third edition of the MSI, and each year we've seen the number of companies admitting to suffering a mobile-related compromise grow.

How much of this can be attributed to increased activity and improved success rates of cybercriminals, or companies becoming more aware of when a mobile device is involved, we don't know for sure. But our data suggests that each played a part in the increase.

Percentages that were compromised

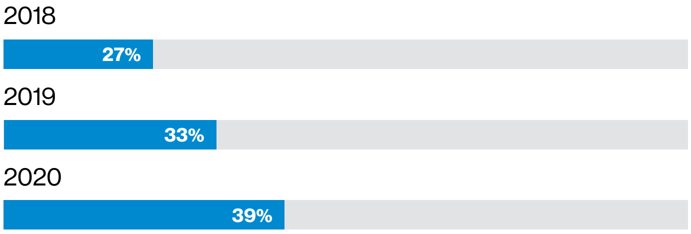


Figure 2. Has your organization experienced a security compromise involving mobile/IoT devices during the past year?

Fewer are cutting corners.

Despite the disappointing increase in the number of companies being hit, we did see a reduction in the proportion saying that they had knowingly compromised security.

However, at 43%, that's still a lot of companies choosing to cut corners and putting their data, their customers' information and their key business systems at risk.

Percentages that sacrificed security

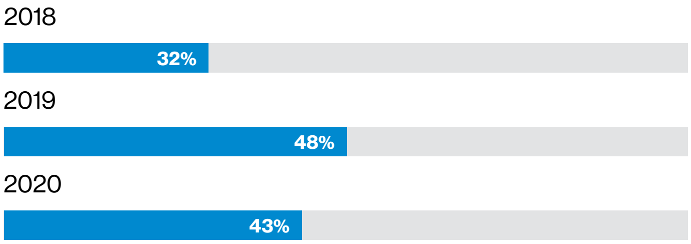


Figure 3. Has your organization ever sacrificed the security of mobile devices (including IoT devices) to "get the job done" (e.g., meet a deadline or productivity targets)?

Back to table of contents >

Speed outweighs security.

This year, we added questions to find out why companies are knowingly exposing themselves to risks. The need to meet targets was the most commonly stated reason, whether it was time (62%) or money related (46%).

Convenience also came in the top three. This mirrors previous findings that showed a willingness to sacrifice "cumbersome" security processes for the sake of streamlining operations. Lack of budget and expertise trailed way behind.

It seems that many companies still see mobile security as an impediment to their business objectives rather than a business imperative in itself. But attitudes are changing. Eighty-seven percent of respondents said they were concerned that a mobile security breach could have a lasting impact on customer loyalty,[1] and 81% said that a company's data privacy record will be a key brand differentiator in the future.

Who is suffering?

Everybody. All verticals were hit, from manufacturing (41% suffered a mobile-related compromise) to the public sector (39%). And companies of all sizes were hit—from small and medium-sized businesses (28%) to those with over 500 employees (44%).

Those that were hit felt the pain.

Two-thirds of those that suffered a mobile-related compromise said that the impact was major.

But it isn't just the immediate consequences that companies need to worry about. The effects included downtime, damage to reputation and regulatory penalties. Fifty-five percent of those that said the compromise was major also said they suffered lasting repercussions.

Information, media and publishing companies, as well as financial services companies (both at 53%), were the most likely to say that the impact of the compromise was major, with lasting repercussions. These industries are particularly susceptible to damage to their reputations.

And putting it right took time and money.

Thirty-seven percent of respondents said that the compromise that they experienced was difficult and expensive to remediate. Retailers were the most likely to feel this, with 61% agreeing.

Reasons for sacrificing security

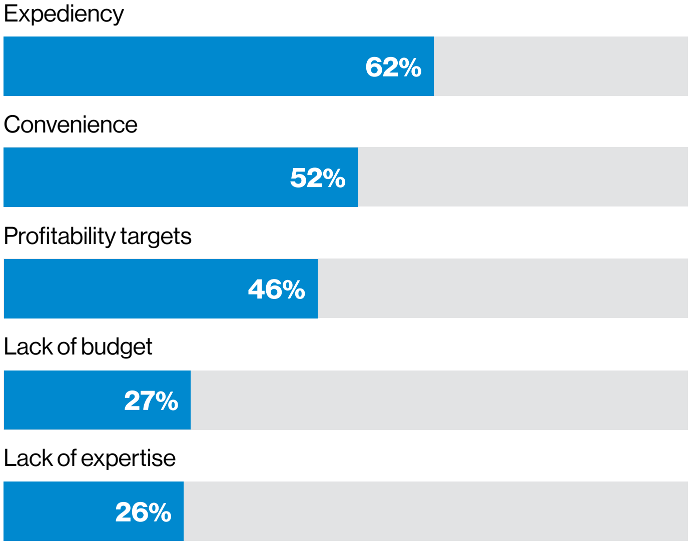


Figure 4. Which of the following drove you to sacrifice mobile security?

Impact of being compromised

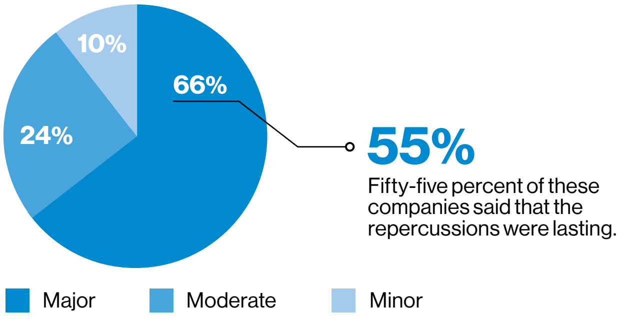


Figure 5. If your organization suffered a security compromise, how serious was the impact? If the compromise was major, did this involve lasting repercussions?

Those compromised more likely to significantly increase spend

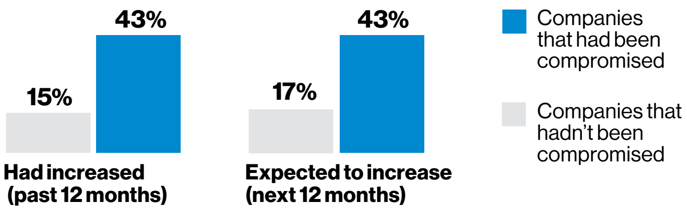


Figure 6. Companies past and future mobile devices security spending, split by whether they'd suffered a mobile-related compromise or not. Those that had described increase as significant.

Back to table of contents ›

What's driving change?

Experience

Unfortunately, for many organizations, the story is, "Get hacked, improve security." In the past year, 43% of companies that had suffered a compromise had also significantly increased their mobile security spend. That number fell to 15% for those that hadn't been compromised. By waiting until their fingers are burned, companies are putting their customer and business data at risk.

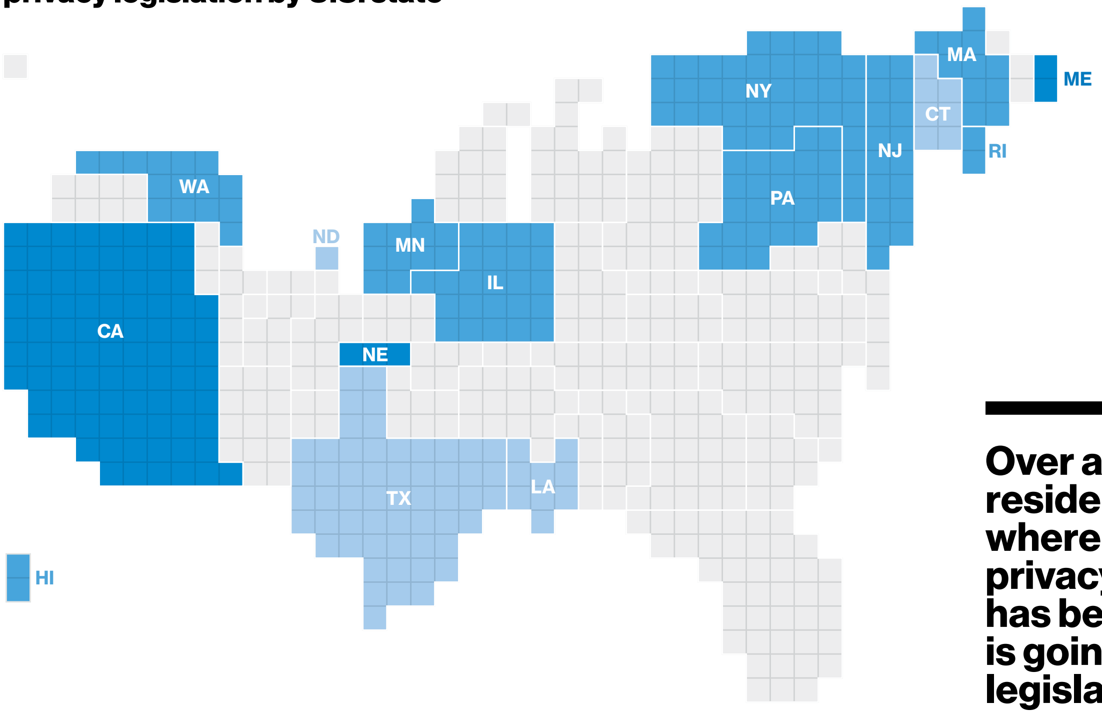
Regulation

If companies aren't going to be proactive, it increasingly looks like governments and industry bodies are going to force their hands.

Following the passage of the EU's General Data Protection Regulation (GDPR) in 2016 and California's Consumer Privacy Act in 2018 – they came into force in May 2018 and January 2020, respectively – there's been increased momentum behind comprehensive privacy legislation worldwide. In the U.S., several states, from Hawaii to Rhode Island, have initiated such legislation. Four other states, including Texas and Louisiana, have set up task forces to look into the issue – see Figure 7.

Twenty-nine percent said they'd suffered a regulatory penalty as a result of a mobile-related security compromise.

Passage of comprehensive privacy legislation by U.S. state



■ New law enacted ■ New bill introduced ■ Task force set up

Figure 7. Each square represents a population of 500,000 people based on 2019 estimates, rounded to the nearest 500,000. Based on analysis by the International Association of Privacy Professionals.[2]

Over a third of U.S. residents live in a state where comprehensive privacy legislation has been enacted or is going through the legislative process.

To be considered comprehensive, legislation must include protection for citizens and obligations on organizations. Rights for data subjects include the right to access, the right to be forgotten (data deletion) and the right of correction. Duties placed on organizations include strict opt-in rules, mandatory notification of data breaches and limitations on processing data–including being transparent with subjects about how you will use their data.

Only 33% of companies said that regulatory penalties are a consequence they are worried about, but that could be because governments have given them adequate time to prepare. Sixty-seven percent said that increased regulation had driven them to spend more on security as a whole.

2

The mobile threat landscape

The usual suspects—phishing, ransomware and malware—remain a worry, but cybercriminals aren't standing still. They are getting increasingly creative at finding new ways to fool users, break through companies' defenses and compromise organizations' systems and cloud-based apps.

verizon

More organizations were hit.

Compiling the data for this report, we found that 39% of organizations admitted to suffering a security compromise involving a mobile device – up from 33% in the 2019 report and 27% in our first report.

Again, the consequences of mobile compromises were shown to be severe and far-reaching. Of those that had suffered a compromise, 66% said the impact was major and 36% said it had lasting repercussions.

A mobile security breach can have serious financial implications and do lasting damage to your brand. And it's not always easy to bounce back. Thirty-seven percent of those that were hit said that remediation was difficult and expensive.

> **Mobile devices have rapidly replaced the personal computer at home and in the workplace. Our phones or tablets are in fact mini-computers, and should be protected as such. They face the same or even more threats than a PC or a laptop.**
>
> — Europol[3]

Consequences of mobile-related compromise

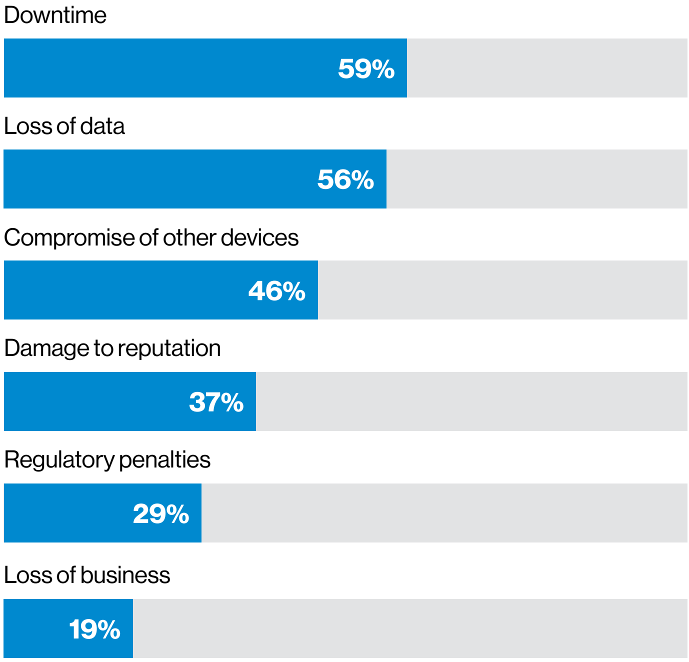


Figure 8. Which of the following consequences did your organization experience as a result of that security compromise?

It's not just your data at risk.

When most people think of cybersecurity compromises, it's the loss or exposure of data that springs to mind. But it's much more than a company's sensitive information that's at risk. A mobile security compromise can have a range of other consequences, including downtime, supply chain delays, lost business, damage to reputation and regulatory fines.

In fact, among those in our survey that had experienced a compromise, downtime was even more common as a consequence than loss of data.

Financial services companies were particularly concerned about this – 95% said that their customers expect a reliable service and that even a few minutes of unplanned downtime could have an adverse impact on the company's reputation.

User threats

Whether they're deliberately breaking policy or inadvertently opening up vulnerabilities, users are a target. Social engineering remains one of the most powerful tools in the cybercriminal arsenal. And attackers are finding increasingly innovative ways to exploit and manipulate users.

Phishing

Year after year, phishing tops the lists of the most common attack types. The 2019 edition of Verizon's annual Data Breach Investigations Report (DBIR) found that 32% of confirmed data breaches involved phishing.

Phishing has been around since the mid-90's. While some of these infected emails are now automatically blocked by mail systems like Google Gmail and Microsoft Office 365, many still get through. And as email providers and the vendors of tools that block phishing evolve, hackers are continually innovating, developing new techniques to evade detection and lure hapless users into divulging valuable information. As a result, the incidence of phishing attacks remains high.

Attacks are becoming more sophisticated and targeted. And as defenses improve, attackers are increasingly turning to mobile.

When you look at your emails on a mobile device, you're at a disadvantage. It's not as easy to spot the signs of something nefarious. You can't always see the padlock symbol or lack of it, or hover over a link to see the underlying URL. This can make users more prone to phishing attacks.

In fact, even among companies with defenses in place – including mobile device management (MDM) and almost certainly at least one form of email filtering – many of their users still received and clicked on phishing links.

And of the users who fell for a phishing attack, most were repeat victims. More than half (53%) of users that clicked on a phishing link clicked on more than one. But according to Lookout's research, enterprise users did better than consumers – the averages being 3.3 and 9.3 times, respectively.[5]

Every day, 2% of employees will click on a phishing link.[4]

Users that fell for one phishing link often fell for many.

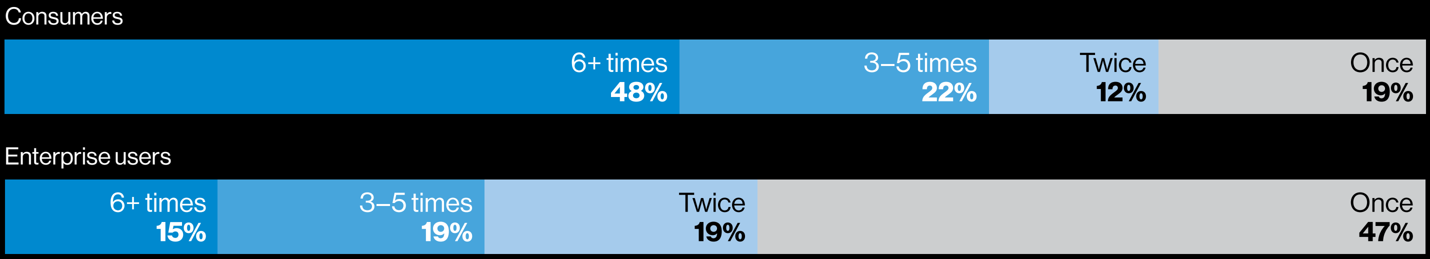


Figure 9. Number of phishing links clicked on by users who clicked at least one link. Data supplied by Lookout.[6]

Back to table of contents ›

> **The average loss from a bank robbery is about $3,000. The average loss from a successful business email compromise attack is nearly $130,000.**
>
> —U.S. Secret Service[7]

Business email compromise

Business email compromise (BEC) fraud – also known as email account compromise (EAC) or CEO fraud – has grown rapidly in recent years. There's no agreed definition as to what differentiates these attacks from other phishing campaigns, but the key characteristics are that they're highly targeted and the perpetrators are after big bucks. Seriously big bucks.

Unlike standard phishing attacks, where volume is the biggest factor to the size of the payout, BEC attacks require extensive preparation. Fraudsters spend time researching targets so they can make the attack as convincing as possible.

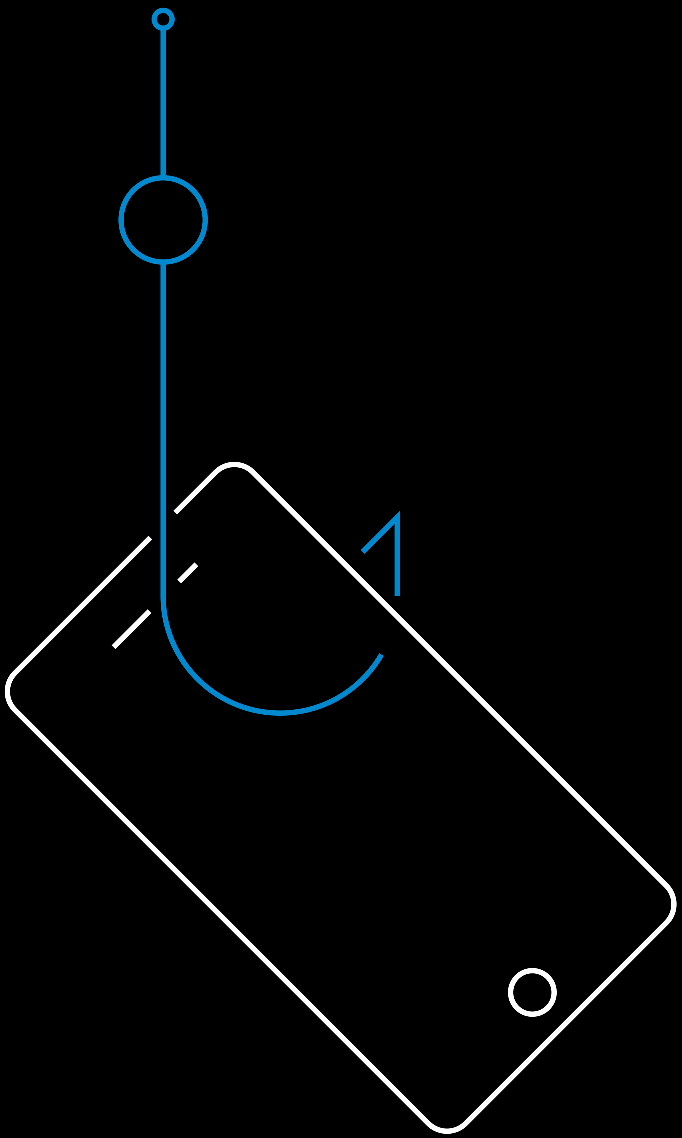
Businesses of all sizes and all types are subject to BEC attacks, and both the frequency of attacks and the damage done are growing. According to the FBI, BEC/EAC incidents have now been reported in all 50 states and across 177 countries. In 2018, the FBI's Internet Crime Complaint Center (IC3) received 20,373 BEC/EAC fraud complaints with adjusted losses of over $1.2 billion. Between May 2018 and July 2019, there was a 100% increase in identified global exposed losses.[8] And that's only incidents where the victim has lodged a complaint to the IC3. There are likely to be many cases that aren't reported.

As with other types of attack, the criminals aren't standing still. While you might be suspicious of an email purportedly from the CFO asking you to transfer a large sum, would you be as wary of a phone call? Attackers are betting that you wouldn't question it. They are feeding recordings of these individuals – often easily obtained online from event videos on YouTube, webinars or social media posts – into artificial intelligence (AI) systems to create deepfakes. With as little as four seconds of audio, a machine-learning (ML) algorithm can create a model that can mimic the person concerned, in real time. This might sound like a movie plot, but advances in AI mean this can be done quickly and cheaply.

Back to table of contents >

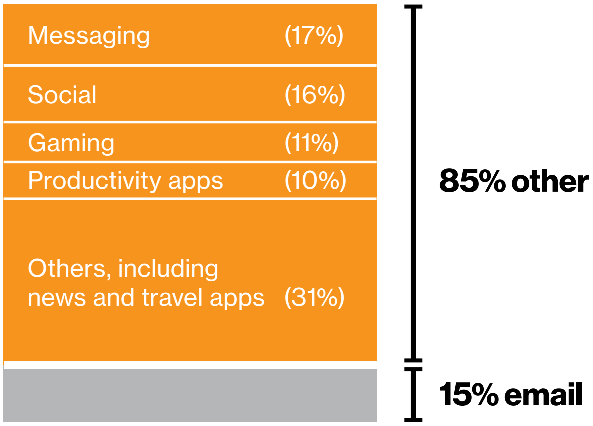
What's the cost of a click?

There are numerous stories of attackers scoring big paydays. In 2019, an employee of a Japanese media company was manipulated into making a $29 M transfer. They were given instructions by a fraudster pretending to be a management executive.



And a town in Florida lost $742 K when one of its accountants fell prey.[9] They received an email claiming to be from a city contractor, which asked them to change an account number. This led to payments going to a fraudster's bank account instead of the legitimate contractor.

When they are successful, attackers quickly transfer the money out of the destination account and it's often very hard to trace it after that.



Phishing type

Figure 10. Prevalence of delivery mechanisms used in mobile phishing attacks. Data provided by Wandera.[12]

Beyond email

When it comes to phishing, it's not just emails that organizations need to be wary of. Eighty-five percent of attacks seen on mobile devices now take place via other mediums.[10] While many organizations have filtering in place to block email-based attacks, far fewer have similar protection in place for these other vectors.

It might seem unlikely, but employees really do fall for SMS phishing attacks. When a large global food distributor sent executives an SMS that looked like it was from a hotel they were due to check into, 54% tapped on the link.[11]

Ways hackers obfuscate phishing links

1. **Use a different top-level domain,**
   e.g., company.net (instead of company.com)
2. **Use homoglyph/punycode,**
   e.g., cømpany.net or xn--cmpany-bya.com
3. **Use what looks like an official domain,**
   e.g., company-support.com
4. **Add detail to confuse,**
   e.g., company.com.supportservic.es/new-password

The use of punycode in phishing attacks is up from around 5% in our last report to 7% in the latest data.[13]

Hiding malicious URLs from users

Mobile users are getting savvier when it comes to spotting suspicious-looking URLs. So hackers are finding new ways to disguise them. Some of the more obvious approaches include using a different top-level domain, or a URL very similar to the company's real address.

One of the more creative approaches involves using punycode, a special type of coding developed to handle non-Latin characters in domain names. It uses combinations of the letters A–Z, 0–9 and the hyphen to represent characters from sets such as Cyrillic (like Б and Д) and Kanji (like 水 and 木). This is useful because it makes the web more accessible to users around the world, but hackers have found a way to exploit it.

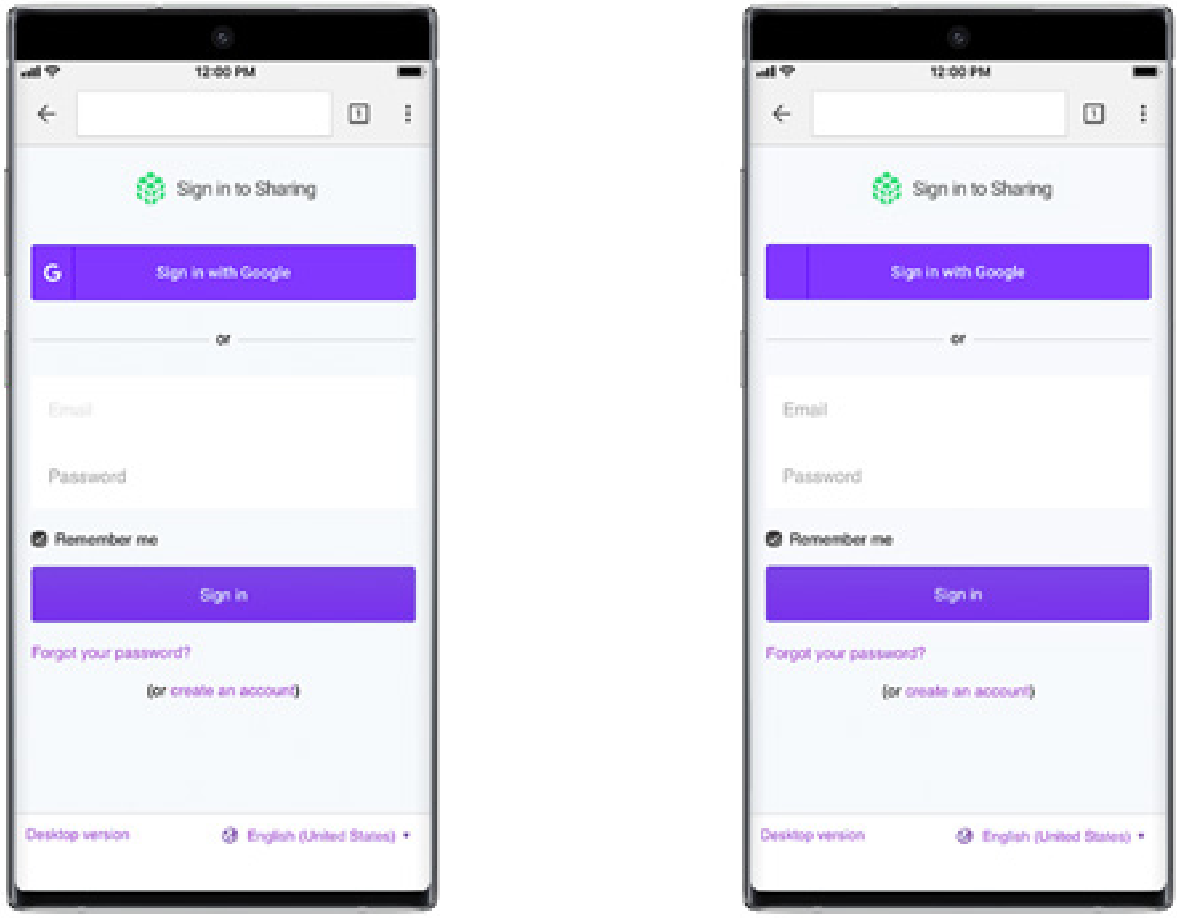
Some of them deliberately use punycode in domain names, knowing that many computers won't have the non-Latin characters available in their default fonts. This means that the punycode converts back to the closest Latin characters instead. For example, most browsers using fonts designed for languages like English, Spanish, French, etc., will display xn--rolx-nu5a.com as rolex.com. The user can't tell that anything out of the ordinary is happening, but the URL is not what it seems.

A similar technique is using homoglyphs: letters that look very similar and could easily be overlooked by a busy user, especially one using a small screen – bìgbank.com, for example, looks a lot like bigbank.com (the lowercase "i" has a grave accent instead of a dot, in case you didn't spot the difference).

Spot the difference.

When the address bar disappears to hide the URL, these two login pages are virtually identical on mobile.

While hackers are getting better at disguising malicious URLs, sometimes the mobile device does the hard work for them. Many smartphones hide the address bar when the user opens a browser window. In the example below, you'd be very unlikely to spot the difference without looking at the link.



Real

Malicious

Figure 11. An example of a real app webpage compared to a fake one seen in the wild. Both images have been anonymized, but are otherwise unaltered. Source images supplied by Lookout.[14]

Example of a simple substitution cipher

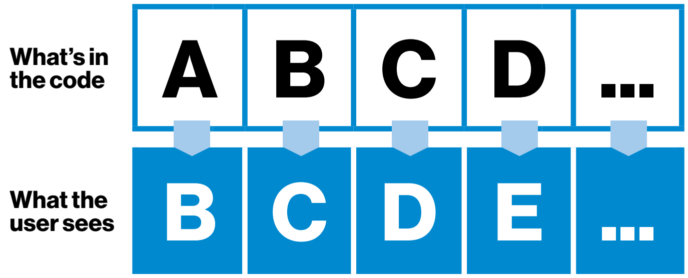


Figure 12. An example of a simple substitution cipher. Each letter in the top row is replaced by the corresponding one below.

Hiding malicious text from scanners

Fewer and fewer companies now manage their own mail servers. It's common for even the largest enterprise to use a web-based email system like Google G Suite or Microsoft Office 365. One of the benefits of these systems is the powerful spam and phishing filters they use – processing email from millions of users gives them a lot of data to work with. While increasingly intelligent, many of these systems still rely on scanning the text of the message to detect threats. And inventive hackers are now finding ways around that.

A recent mal-innovation has been the use of a customized font. Using a simple substitution cipher, the attacker is able to split what a human reader sees and what an email scanner (or threat detection app) reads. A malicious message such as "Click to reset your login" would be masked as gobbledygook, like "Bkhcj sn qdrds xntq knfhm," in the underlying HTML. This would help the hacker evade detection and blocking.

Companies where a user accessed inappropriate types of content

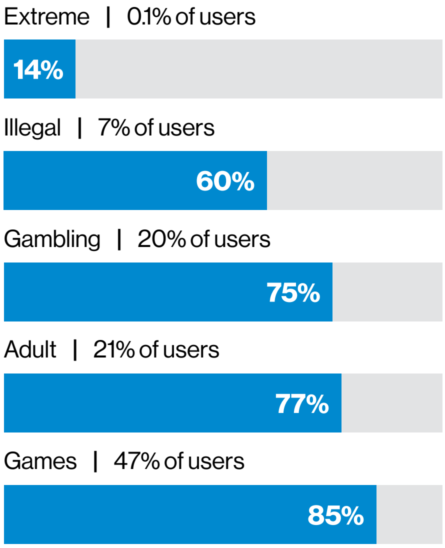


Figure 13. Types of inappropriate content accessed by employees on mobile devices. Data provided by Wandera.[15]

Acceptable use or abuse?

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. And employees often expect a bit more leeway when traveling for work – after all, they are giving up their free time and creature comforts.

Some behavior is clearly unacceptable, such as accessing adult, extreme, illegal or gambling content on company devices. And it's not just because it could damage your company's reputation. These sites are far more likely to harbor malware or other malicious threats.

Our survey found that 72% of organizations were worried about device abuse or misuse, and about one in five (19%) didn't feel prepared for it. Part of the problem is that many companies struggle to develop an effective acceptable use policy (AUP) – 44% didn't have one at all.

Defining what counts as misuse of a work device can be a daunting prospect, especially if your employees need to access social media or consume a wide variety of content. But creating clear guidance, including rules for mobile-specific content, is crucial for preventing misuse.

Ready to develop an effective AUP for your employees?

This guide can help you get started: enterprise.verizon.com/msi-aup

Back to table of contents >

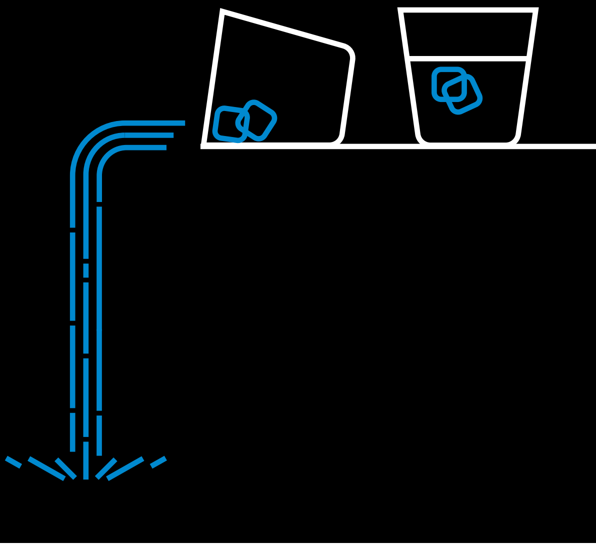
No such thing as a free drink

Attendees of a mobile security event were sent a phishing email that purported to be from the hotel they were staying in, offering them a free drink at the bar. Seventy percent opened it and clicked on the link.[16] This example from VMware shows how easy it is to phish even mobile security experts!

How many conferences offer discounted rates at a preferred hotel? And how many publish lists of companies attending and even the names of speakers? Put these together and presto!

And it's not just the danger of malware-infected sites. Many hotels now offer apps. With mal-innovation happening all the time, it's not hard to imagine a scenario where a user is convinced to install a compromised version. Or they could be fooled into giving away credentials to their loyalty account. This could allow a hacker to install the hotel's app, log in and use the keyless entry to gain access to the person's room.

According to IBM, more than one in seven travelers said they'd had their personal information stolen at least once while traveling.[17]



Excess permissions

The average user or employee could have hundreds of apps installed on a single mobile device, especially if they're using it for both work and personal activities. But how many employees read the full terms and conditions or review permissions for each app before clicking "OK"?

In their rush to install the latest and greatest app, many users willingly grant all kinds of permissions—including access to their camera, microphone, contacts and call log. But how often are these permission requests legitimate? Even with the millions of photo-editing apps that exist, it's hard to believe that 74% of all iOS apps need access to the user's photo library—or that 32% of apps need to use the microphone.

Occasionally there will be a genuine reason for an app requesting superfluous permissions—such as the developer planning to add new features in the future. But even if they have no malicious intent, these unnecessary permissions could be exploited by hackers. For example, access to the camera could be used to spy on the user or capture passwords being entered, while microphone access could be used to eavesdrop on phone calls. Even contact lists can be exploited and used to send targeted phishing emails.

Permissions granted

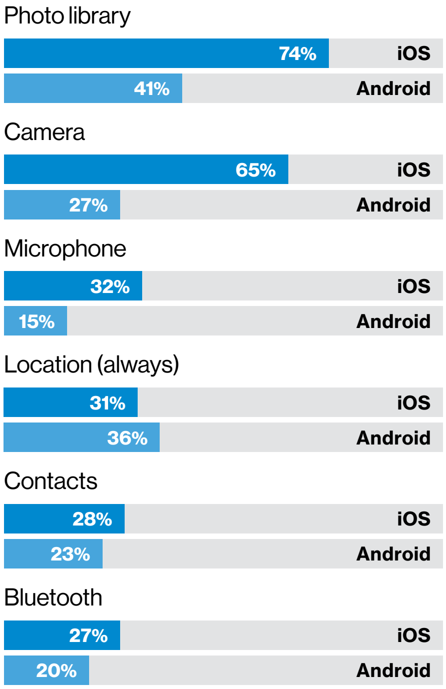
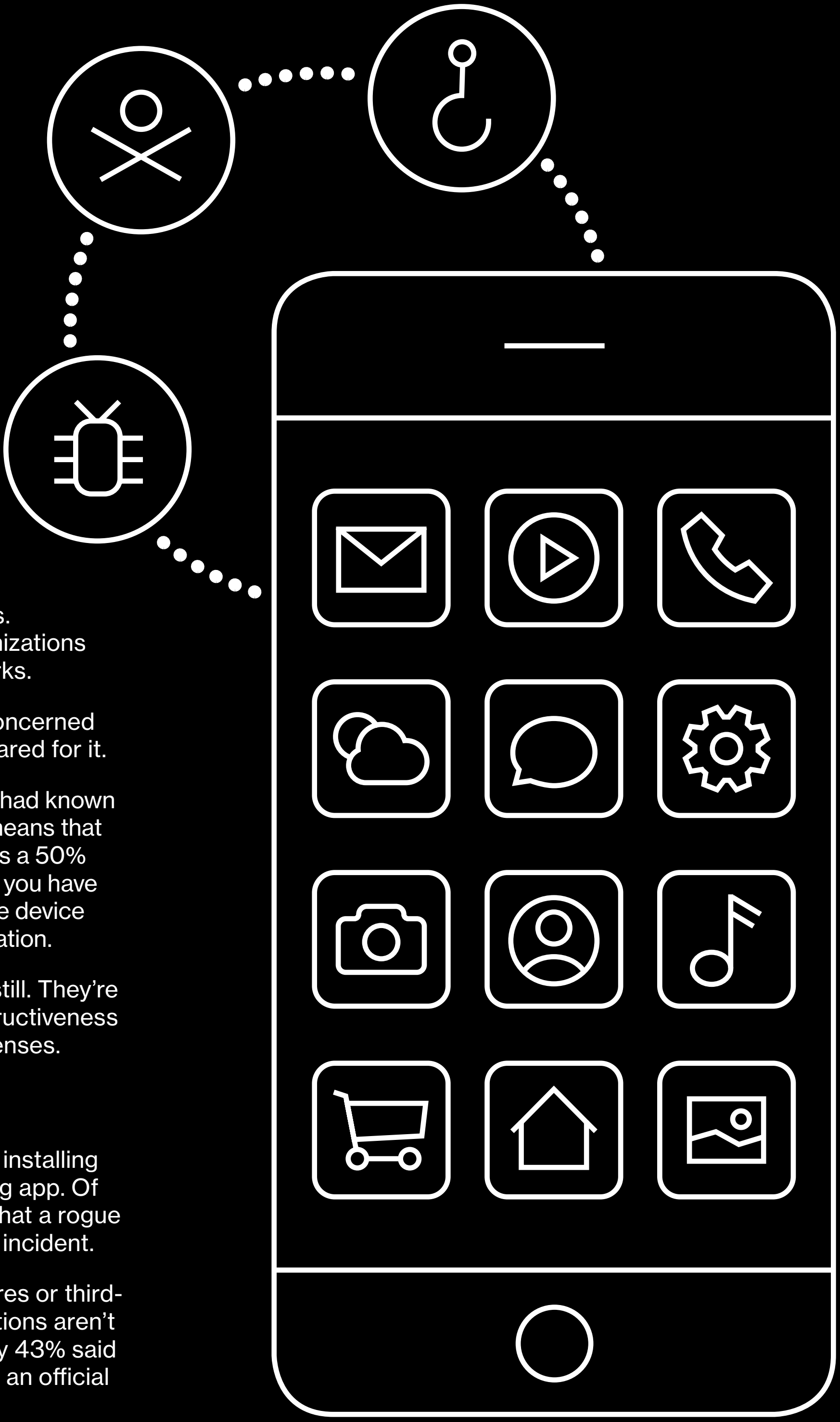


Figure 14. The permissions granted to apps on iOS and Android devices. Based on analysis of 53 million apps installed on devices in production use.[18]

Back to table of contents ›

App threats

Well-known problems like malware and ransomware remain major threats, but emerging ones like cryptojacking can also put your organization at risk. Even apps downloaded from official stores can be compromised or introduce vulnerabilities due to poor coding practices.



Malware

This remains one of the favorite tools of attackers. It constantly tops our list of the threats that organizations are the most worried about. Why? Because it works.

This year, 86% of organizations said they were concerned about malware, and 20% of those don't feel prepared for it.

According to MobileIron, 4.5% of Android devices had known malware.[19] That might not sound like much, but it means that if your organization has just 15 devices, then there's a 50% chance that at least one of them is infected. And if you have 100 devices, that chance goes up to 99%. And one device can be enough to compromise your entire organization.

As with other threats, criminals are not standing still. They're constantly finding new ways to increase the destructiveness of malware and break through organizations' defenses.

Malware within apps

One of the most effective ways to trick users into installing malware is to disguise it as a useful or entertaining app. Of organizations that were compromised, 21% said that a rogue or unapproved application had contributed to the incident.

Of course, sideloading apps from non-official stores or third-party websites increases the risk. Many organizations aren't regulating where apps are downloaded from. Only 43% said that they limit their employees to using apps from an official app store or one owned by the company.

Back to table of contents ›

And hackers are getting smarter, using more sophisticated techniques to make malicious apps look legitimate. There have been numerous instances of malware-infected apps escaping detection and being spread through official stores like Google Play. Official app stores have thousands of apps to test and approve, and some malicious ones inevitably slip through the cracks. And because testing tends to be more rigorous on the first version, some attackers sneak malware into approved apps via updates.

"Elusive" malware

How effective a piece of malware is isn't just dependent on how damaging it is. Whether they are stealing credentials or enlisting devices to their botnet, hackers want their malware to infect as many devices as possible.

And hackers are learning a lesson from biological diseases. Some deadly illnesses don't tend to spread very far due to high mortality rates, limiting their overall impact on a population. By contrast, illnesses like the common cold or flu have a slower onset of symptoms. This longer incubation period gives infected people time to catch planes and trains and spread the disease.

Elusive malware operates in a similar way. It will stay completely dormant on a device for a period of time – weeks, or even months – until it's triggered. Because the malicious part of the app hasn't been activated, the app can gather good reviews (or have them paid for) and users may recommend it to friends and colleagues, helping it spread to many more devices.

The trigger for the malicious part to spring into action may be as simple as reaching a particular date – reminiscent of early "time bomb" viruses. But criminals are getting increasingly sneaky. There are examples of malware being programmed to trigger after a set number of steps are taken, identified by the onboard accelerometer. This makes it harder for security researchers to spot the malicious code, as tests are normally conducted on lab benches or even in PC-based emulators.

> **"**
>
> **The growing availability of ready-made malware is further creating opportunities for even inexperienced criminal actors to launch their own operations.**
>
> —U.S. Secret Service[20]

Back to table of contents ›

> **“The number of reported ransomware attacks has decreased, but the loss amount has significantly increased. More money can be extorted from a business—especially a large, profitable one—so hackers are moving from targeting personal devices to corporate owned/controlled ones.**
>
> —FBI[21]

Ransomware

Ransomware remains one of the biggest mobile device security threats, but it’s also one that companies feel the most ready for–85% said they are worried but 76% of those felt prepared. This is probably because ransomware has been getting a lot of media coverage, particularly recent attacks on the public sector where city systems have been held for ransom. This awareness has driven many companies to ramp up their defenses. This supports our observation that many companies wait until they themselves, or organizations they know, are hit before taking action to improve their defenses.

But they may not realize how fast ransomware is evolving. The early versions simply locked the files on your device. Newer variants lock the files you have stored in online services like Google Drive and Office 365. An even more alarming variation is doxware, which instead of encrypting your personal files threatens to publish them online.

Insecure coding

You might only be using apps from the most trusted, reputable companies, but in the rush to get updates out, even they can deploy apps with vulnerabilities. Seventy-five percent of organizations said they were concerned about this threat, and 23% of those didn’t feel prepared for it.

There’s also the risk of stealers to contend with. Many users take advantage of built-in browser features that save your passwords. But now, malicious malware apps are being created that can interact with your browser and exploit the way this feature has been coded. Originally, these apps were created to compromise cybercurrency wallets, but attackers are now using them to steal user credentials. This could enable them to get into both personal accounts–like banking and shopping accounts–and corporate resources.

Back to table of contents ›

Relative volume of cryptojacking attacks versus value of cryptocurrency

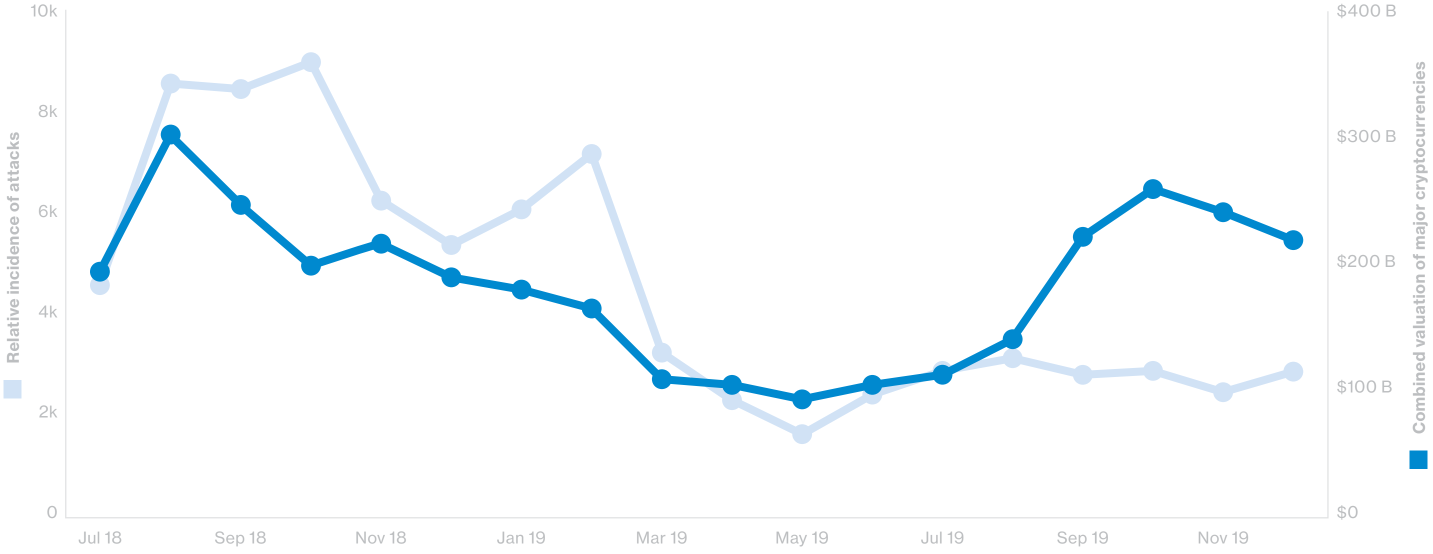


Figure 15. Relative incidence of cryptojacking attacks and value of major cryptocurrencies, one month offset. Data provided by Wandera.[22]

Cryptojacking

Cryptojacking is the unauthorized use of a device to mine cryptocurrency. As we showed in our previous report, thanks to an experiment carried out by Wandera, it can significantly drain the battery life of devices. And this can lead to bigger problems, like downtime or operational disruption. Although cryptojacking is a relatively new threat, 73% of organizations said they are concerned about it.

Working with Wandera, we analyzed the volume of cryptojacking attacks and the major cryptocurrencies. We found some correlation (r^2 = 0.26) between the market value and the number of attacks, with a lag of about three months. This analysis is very simple, but does suggest the value of cryptocurrencies has some impact on the volume of attacks. Of course, there are many other factors influencing a hacker's choice of method of attack.

Patching apps

Many companies are not regulating which apps their employees are using – only 62% have banned the installation of unapproved apps within their AUP.

And the problem isn't just which apps employees are using, it's how many of them. A single mobile device can have hundreds of apps installed, each potentially a source of vulnerabilities. That makes it harder to keep them all up to date.

There are many reasons why users fail to patch their apps: They might have their device set to wait for Wi-Fi access to perform large updates, or they may simply be avoiding the hassle of updating. Setting updates to run automatically in the background can avoid some of these problems, but an untested update could introduce problems itself.

What's up?

On May 12, 2019, the makers of WhatsApp announced that users had been subject to a spate of attacks where hackers exploited a buffer overflow vulnerability to run malicious code. When the culprit called the victim, the code would be executed and the device infected – even if they didn't answer. Some attacks installed surveillance tools on the device, enabling the attacker to eavesdrop on conversations and track movements.

The company urged its 1.5 billion users to install a new patched version immediately. But despite the seriousness of the vulnerability, users were remarkably slow at doing so. Even after six months, more than 1 in 15 users hadn't updated and remained susceptible to attack.

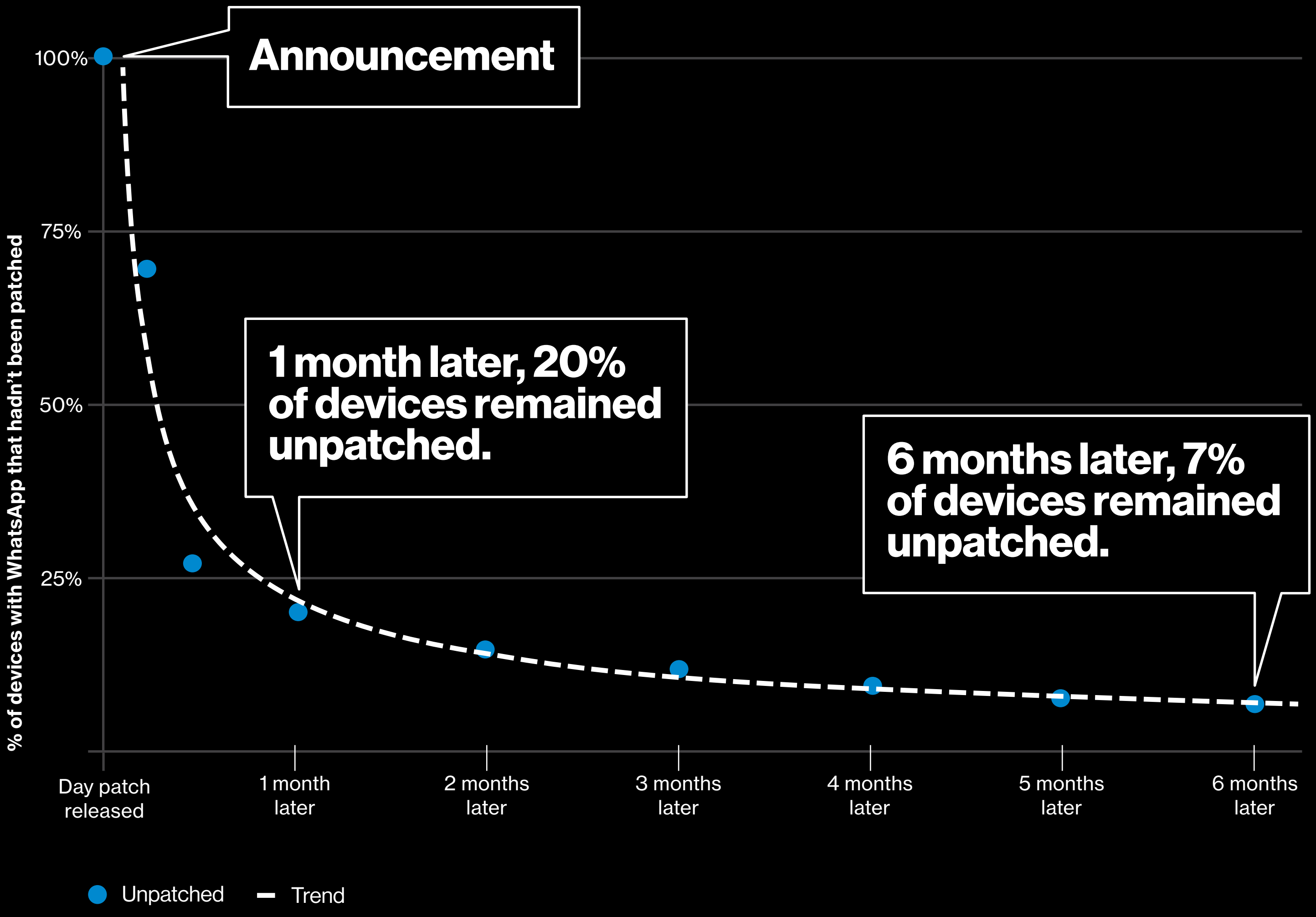


Figure 16. Percentage of devices with an unpatched version of WhatsApp installed, out of all those with the app installed. Data provided by Wandera.[23]

Back to table of contents ›

Device threats

Lost or missing devices are a fact of life for most organizations, yet many companies still fail to use whole-disk encryption. And then there's the challenge of keeping all devices patched and updated.

31%

According to MobileIron, 31% of devices were found to harbor known threats. That's almost unchanged since 2018.[24]

This year, our study looked at businesses of all sizes, 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 OS vulnerabilities.

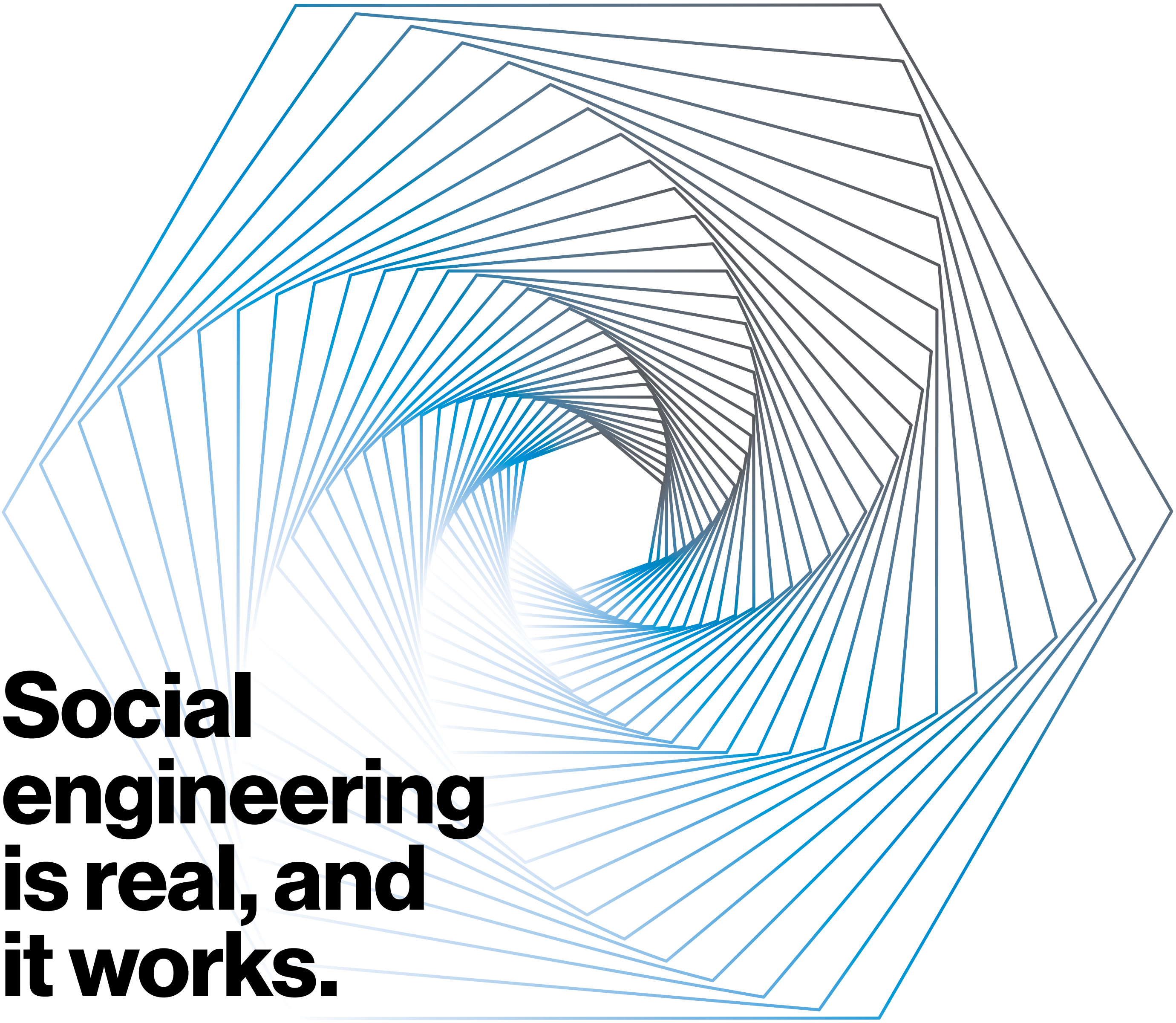
SIM swapping

Imagine your mobile phone suddenly displayed the message "no network"; what would you think? You'd probably roll your eyes and blame your provider. You might try shifting location, and when that fails, go for the dreaded restart. What if it still isn't working? Would you suspect that somebody had hijacked your number and was now getting all your texts and calls? You might think that a bit of peace and quiet would be a nice change, but remember that those messages might include two-factor authentication texts and calls about resetting passwords.

SIM swapping involves an attacker researching the victim to gather personal details like their date of birth and address. They then call up the mobile phone provider, impersonating the victim, and ask to transfer the target phone number to one owned by the attacker.

It's a growing threat. Based on the number of incidents reported to the FBI's IC3 unit, the number of successful attacks has almost doubled year-on-year since 2016.[25]

Back to table of contents ›



Social engineering is real, and it works.

Many people think they won't fall for social engineering, but it doesn't always take place over email or the phone. You never know who might be watching you in public. Imagine you're sitting on a train with your laptop and a coffee. The coffee cup has your name on it, and your company's logo is visible on your desktop. With just those two pieces of information, a hacker sitting behind you could do a frightening amount of recon.

It only takes a quick search using those two bits of information for the hacker to find your LinkedIn page with a list of your colleagues and workplaces, past and present. Maybe it will also bring up an Instagram or Facebook page, or if not yours, then somebody else's that mentions you—for example, in a caption: "Dave at the XYZ company Christmas party."

The hacker won't be interested in your family photos, but what about your contacts? Your grandmother's surname is your mother's maiden name. And what about your child's birthday or the date of your wedding anniversary? These are often used to create "stronger" passwords.

Physical access

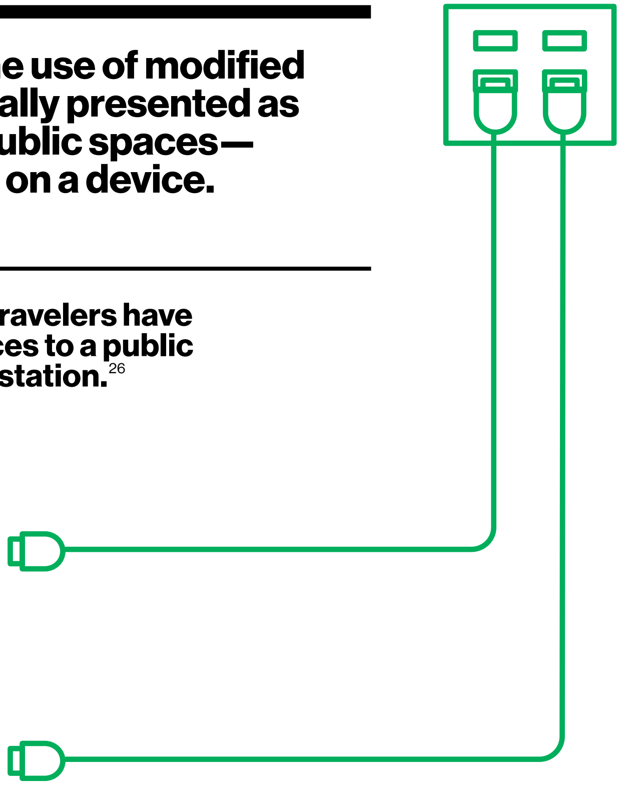
The vast majority of attacks don’t depend on physical access to the device. But if attackers can get it, access opens up a lot of opportunities to do damage.

Even just a few minutes of physical access to a mobile device is enough to install something malicious, such as stalkerware. This is readily available on the internet and allows the attacker to eavesdrop on everything the victim does: emails and text messages they send and receive, photos they take, where they go. Attackers can even watch and listen to victims through the device’s camera and microphone.

The office environment is normally seen as a safe zone, with laptops and other devices often left unattended. With many people working in open-plan offices and hot-desking, this provides lots of opportunities to insert something malevolent into a port. Stalkerware might also be used by an abusive partner or other individual. While poking into work files might not be the primary motive, it would likely be enough to break compliance rules.

Juice jacking is the use of modified USB ports—typically presented as free charging in public spaces—to install malware on a device.

IBM found that most travelers have connected their devices to a public USB port or charging station.[26]



63%

Personal travelers

79%

Business travelers

Loss and theft

Everybody loses stuff, including expensive devices packed with valuable information. They leave devices in taxis, on trains, at restaurants – the list goes on and on. Some of these will end up in lost and found, others will find a new owner.

Some 83% of organizations said they are concerned about device loss/ theft, and 20% of those felt that their defenses were inadequate to deal with this threat – despite it being one of the easiest types of attack to prepare for and mitigate. Encryption and remote wipe are now standard with many common user devices, but that doesn't mean that companies are using them.

These are basic precautions that don't cost a dime but could prevent a device that falls into the wrong hands from leading to a compromise.

IoT devices

The volume and variety of connected devices is growing rapidly. Eighty-four percent of organizations said that IoT devices are crucial to their digital transformation. What are the risks of IoT, and how can your organization stay prepared? We explore the state of IoT device security starting on page 54.

37%

Only 37% of companies in a VMware customer survey said they were using whole-disk encryption (WDE) on laptops.[27]

5%

According to Symantec's latest data, 5% of enterprise devices don't have encryption enabled, down from 11% the previous year.[28]

2%

Two percent of corporate and 6% of all devices using Wandera's device management didn't even have a lock screen enabled.[29]

Out-of-date operating system (OS)

It's not just the major OS updates that matter. Threats are evolving all the time. Missing an update, even a minor one, can put mobile devices at greater risk. How many people can honestly say that they've never clicked "Remind me later" when asked to update? Can you?

There are several factors driving the lag between OS updates being released and users installing them. First, device replacement cycles are growing. Just a few years ago, people were queuing around the block to upgrade to the latest iPhone. But devices are now extremely advanced and innovations less dramatic – typically, most new features are software and hardware updates focused on improvements to cameras. With fewer "must have" advancements, many owners are prepared to hold on to their devices longer.

Second, many software updates aren't that compelling for users. Often, they only bring minor changes to functionality. Since users know they're not going to experience much of a difference, they may think the hassle of upgrading isn't worth it and delay it as long as they can.

There are many other reasons that updates are sometimes delayed, including device settings. For example, many devices have a setting to wait until the user is connected to a Wi-Fi network to execute updates over a set size, and most OS updates are quite big.

But many companies aren't taking advantage of the update policies that are built into their managed Android devices. According to IBM data, almost half (49%) of enterprise devices are being used without any managed update policy – the decision to update is being left up to employees. Just 21% of these devices are set to immediately install system updates – see the chart below.

Update policy on managed enterprise Android devices

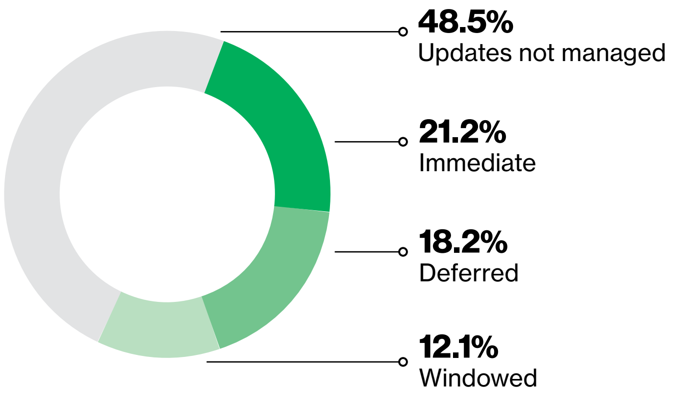


Figure 17. Immediate – installs all system updates as soon as they become available, without user interaction. Deferred – allows the user to defer system updates for up to 30 days. After this, the user is prompted to install the update. Windowed – automatically installs all system updates during a prespecified daily maintenance window.[30]

CVEs* by version (Android)

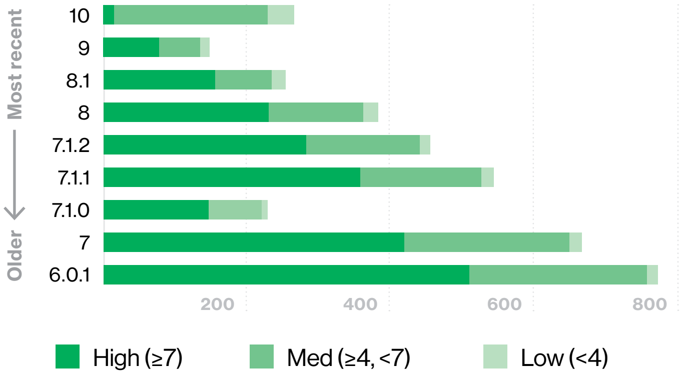


Figure 18. Version number of Android and corresponding number of *Common Vulnerabilities and Exposures (CVEs)[31]

CVEs* by version (iOS)

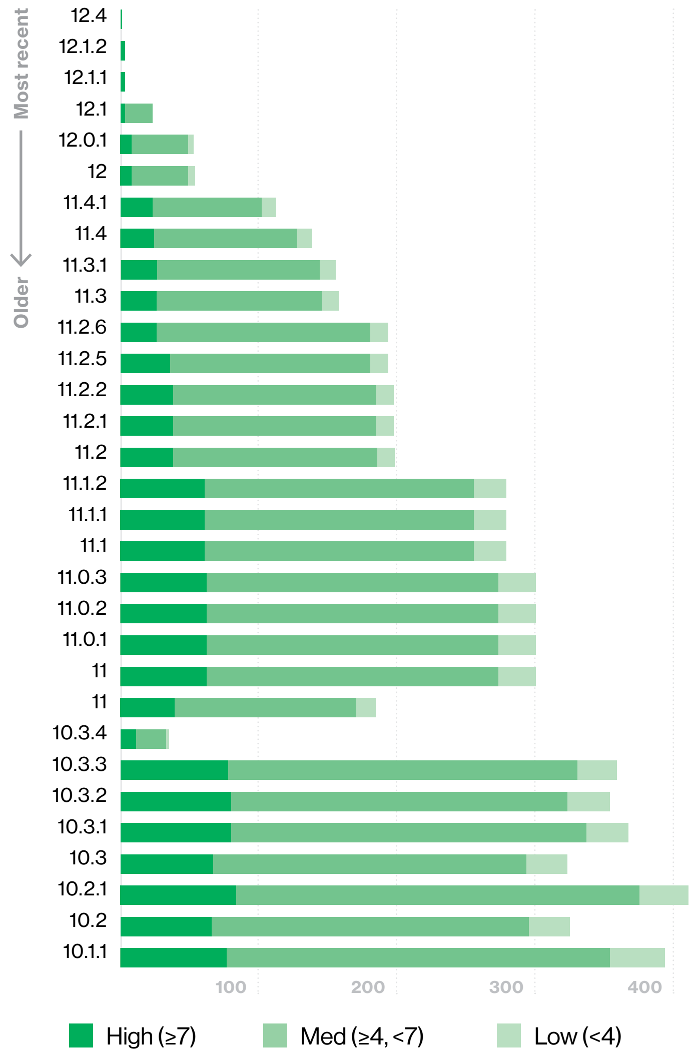


Figure 19. Version number of iOS and corresponding number of *Common Vulnerabilities and Exposures (CVEs)[32]

Back to table of contents >

Network threats

Insecure networks remain a serious mobile device threat. Attackers can intercept traffic through man-in-the-middle (MitM) attacks, or lure employees into using rogue Wi-Fi hotspots or access points.

Use of public networks

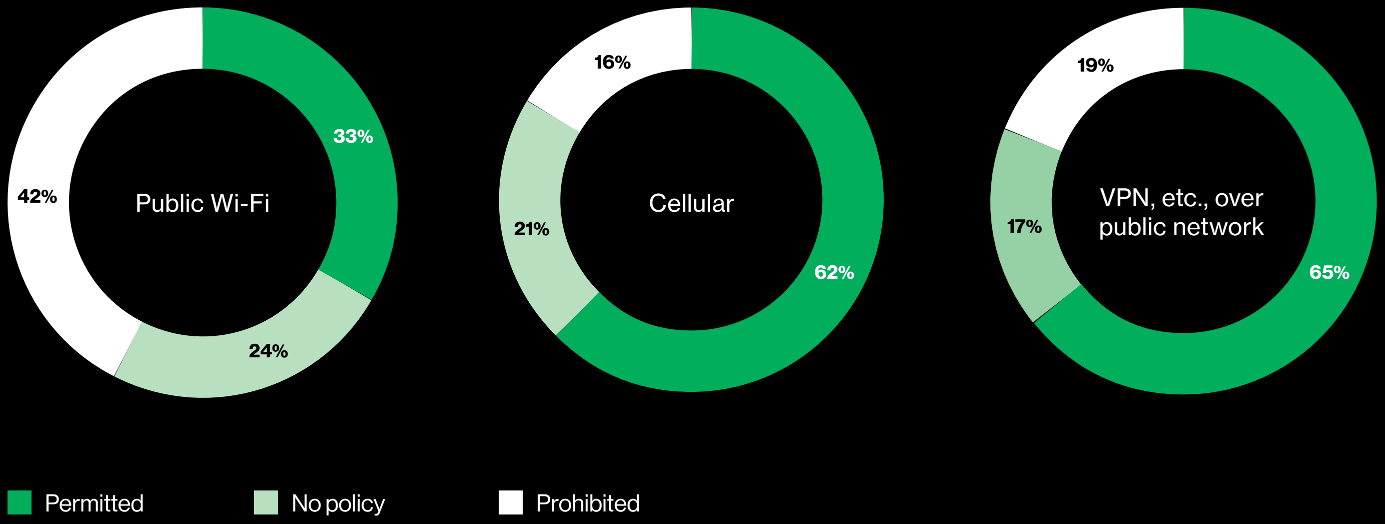


Figure 20. Which of the following are your employees allowed to use for performing work-related tasks?

Back to table of contents ›

According to MobileIron, 7% of protected devices detected a MitM attack in the past year.[33]

Although the risks of public Wi-Fi are becoming well known, convenience trumps policy—even common sense—for many users. Some organizations are trying to prevent this by implementing Wi-Fi-specific policies, but inevitably, rules will be broken (see page 34 for more info).

One of the most dangerous network threats is the interception of traffic, or MitM. This is often done through rogue access points, which take advantage of familiar and trusted public Wi-Fi names (SSIDs). Users may see the name of a legitimate company or brand and connect to it without a second thought.

While some rogue hotspot names are obviously misspelled (e.g., Starbuckz), many look perfectly legitimate. And users might have the access point already stored in their device, causing it to connect automatically.

That might sound like something out of a spy movie, but it's more prevalent than SQL injection (SQLi)-type attacks, and almost as common as phishing—but it gets far less press; maybe it needs a better agent?

Seventy-two percent of organizations said they're concerned about MitM attacks. Of those, 23% don't feel prepared.

Attempts to exploit misconfigured servers, including SQL injection (SQLi)-type attacks

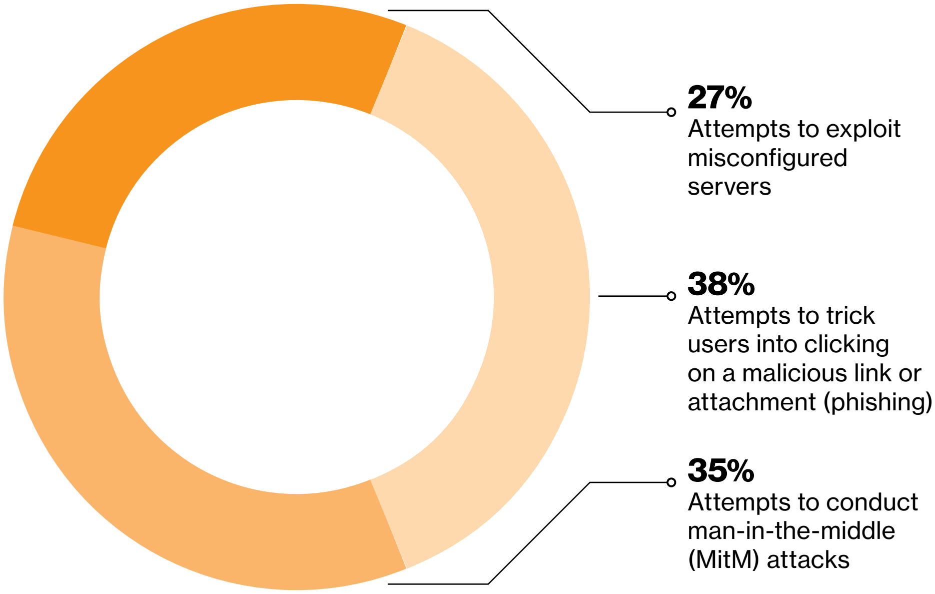


Figure 21. Types of exploitation targeting inadvertent weaknesses. Data provided by IBM.[34]

Back to table of contents ›

The dangers of Wi-Fi

Rogue or insecure hotspots

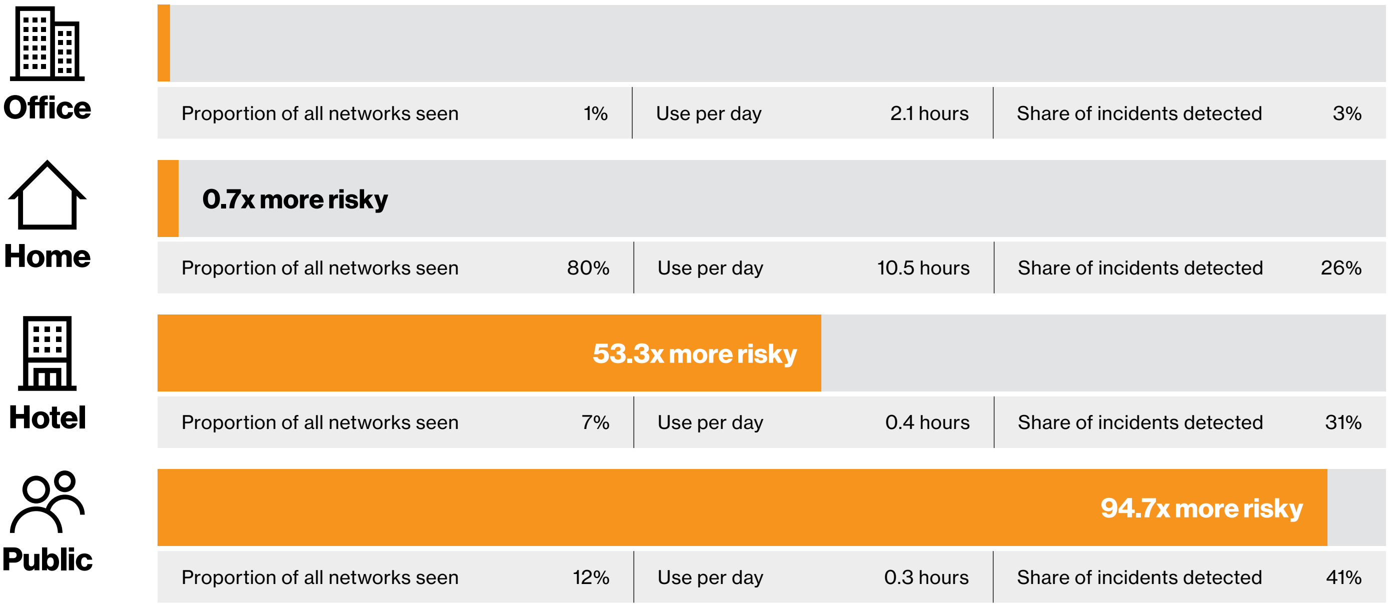
Not all access points can be trusted—even those carrying the name of a trusted business or brand. The risk of insecure hotspots may be greater than companies realize. Twenty percent of organizations that suffered a mobile compromise said that a rogue/insecure Wi-Fi hotspot was involved.

According to Wandera, employees connect to an average of 24 Wi-Fi hotspots per week. It also found that 7% of devices encounter a hotspot that presents a low-to-medium severity risk, and 2% encounter one rated as a high risk—one known to be affected by MitM, or a protocol attack like SSL Strip.[36]

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.[37]

NetMotion data shows that 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, like airports.[35]

Relative risk of different types of Wi-Fi



Office	Proportion of all networks seen	1%	Use per day	2.1 hours	Share of incidents detected	3%
Home	Proportion of all networks seen	80%	Use per day	10.5 hours	Share of incidents detected	26%
Hotel	Proportion of all networks seen	7%	Use per day	0.4 hours	Share of incidents detected	31%
Public	Proportion of all networks seen	12%	Use per day	0.3 hours	Share of incidents detected	41%

Figure 22. Usage and share of incidents by type of Wi-Fi. Data provided by Symantec.[38]

Back to table of contents >

Despite the clear security advantages of cellular technology, Wandera found that mobile workers transfer 2.5 times as much data via Wi-Fi.[39]

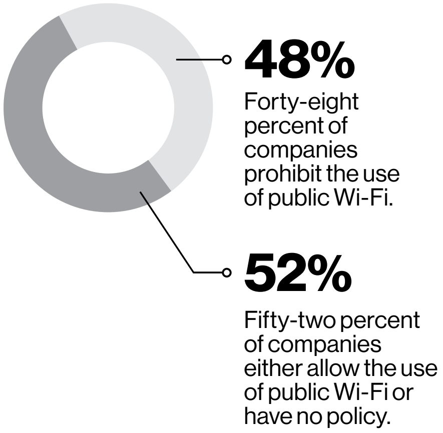
Rules will be broken.

Despite the risks, less than half (42%) of organizations said that they prohibit employees from using public Wi-Fi to perform work-related tasks. But even if they're banned from using it, many employees will break the rules for the sake of convenience. Fifty-five percent of those who know that public Wi-Fi is prohibited use it anyway. And ironically, that includes many who are responsible for managing the security of mobile devices.

This shows the importance of having protection that's built in. By using a system that blocks access to insecure or untrusted networks automatically, you don't have to rely on users always making the right decision.

> **Don't allow your phone, computer, tablet or other devices to auto-connect to a free wireless network while you are away from home. This is an open invitation for bad actors to access your device. They then can load malware, steal your passwords and PINs, or even take remote control of your contacts and camera.**
>
> —FBI[40]

Policy on public Wi-Fi



Employee use of public Wi-Fi

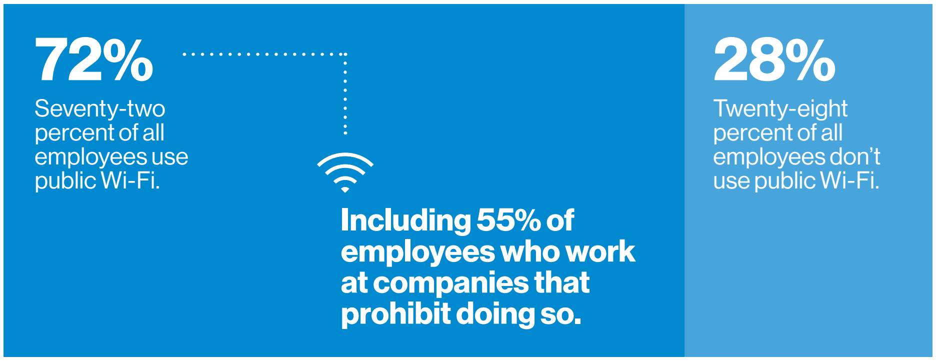


Figure 23. Are your employees allowed to use public Wi-Fi (e.g., in a coffee shop or hotel) for performing work-related tasks? Do you ever personally use public Wi-Fi for work-related tasks?

Back to table of contents ›

Insights by sector

Financial services

47%

Forty-seven percent were compromised.

2.1x

Two-point-one times as likely to be compromised if they sacrificed security

Customers put a lot of trust in their financial institutions, and that means these organizations are under pressure to stay secure. Ninety-five percent said their customers expect a reliable service, and any less could have a lasting impact on their reputation. But they're also at serious risk—87% said that cybercriminals see their sector as a more lucrative target than other industries.

In this year's study, we found that almost half (48%) had sacrificed security in the name of expediency. And cutting corners has taken its toll. The sector was the second most likely to have suffered a mobile compromise (47%), behind information and media. Since financial services companies think that a good cybersecurity reputation is key for attracting customers, they could benefit greatly from reassessing and strengthening their mobile security.

enterprise.verizon.com/msi-financial-services

Healthcare

38%

Thirty-eight percent were compromised.

1.9x

One-point-nine times as likely to be compromised if they sacrificed security

Healthcare organizations are using mobile to empower employees and deliver better patient outcomes. It's helping to improve outpatient care, reduce readmission rates and provide insights to improve the accuracy of diagnostics and treatments.

Despite the benefits of mobile, healthcare organizations are worried. Eighty-eight percent said they are concerned that the highly confidential nature of patient data makes them a target for cybercriminals. And it's more than just privacy that's at risk. Eighty-five percent said they feared that a security compromise could seriously compromise patient care.

Healthcare organizations also face unique challenges when it comes to security. In a clinical setting, employee efficiency and productivity are crucial. The ability to make fast decisions can mean the difference between life and death. Seventy-two percent of organizations said that this need for speed made it harder to implement effective controls.

Thirty-eight percent of those in our latest survey said that they'd suffered a mobile security compromise—a significant increase from the 25% we reported in 2019.

enterprise.verizon.com/msi-healthcare

Information and media

50%

Fifty percent were compromised.

1.8x

One-point-eight times as likely to be compromised if they sacrificed security

In their quest to create the next commercial success, many information and media companies seem to be neglecting mobile security. Seventy-three percent had knowingly sacrificed security – more than any other industry. And 50% had suffered a compromise involving a mobile device. That's a major leap from the year before, when just 33% were compromised.

For these creative companies, protecting intellectual property (IP) is often key to their competitive advantage. Over half (55%) of information and media companies were worried about the exposure of their IP or trade secrets, compared to an average of 42% of all companies.

Despite their concerns, only 1 in 10 are following four of the most basic security precautions – changing default passwords, testing security, encrypting data and restricting access on a "need to know" basis.

Manufacturing, construction and transportation

41%

Forty-one percent were compromised.

1.9x

One-point-nine times as likely to be compromised if they sacrificed security

Companies in this sector know that a mobile security compromise can be disastrous. Eighty-nine percent said that a mobile security compromise could disrupt their entire supply chain, with serious financial implications. And if an attacker gained access to critical systems or disrupted machinery, the consequences could be even worse. Eighty-one percent said that a compromise could threaten the physical safety of their employees.

Manufacturers aren't just worried about falling victim to attacks by random hackers; they're also concerned about which hands their stolen data could fall into. The vast majority (84%) said they are specifically worried about their competitors stealing their trade secrets or IP.

Yet despite everything that's at stake, they're still cutting corners on security: Less than half (45%) said that they change all default passwords or encrypt sensitive data when sending it across public networks (47%). Over two-fifths (41%) suffered a mobile compromise this year, almost twice as many as we found in our previous report.

enterprise.verizon.com/msi-manufacturing

Professional services

27%

Twenty-seven percent were compromised.

2.1x

Two-point-one times as likely to be compromised if they sacrificed security

Professional services companies – including accountants, lawyers, real estate brokers and surveyors – tend to be customer-facing businesses. More than half were worried about suffering damage to their reputation as a result of a mobile security compromise (55%). They were also concerned about a range of data being compromised or exposed – including sensitive internal or strategic data, employee data and customer data – all cited by more than 70% of industry respondents.

Perhaps that's why these companies are playing it relatively safe. Of all sectors, they were the least likely to have sacrificed mobile device security (26%). And their efforts seem to be paying off – they were the least likely sector to have suffered a mobile compromise. Just over a quarter (27%) were hit this year. That's a major improvement on 2019, when over two-fifths (41%) were hit.

Public sector and education

39%

Thirty-nine percent were compromised.

2.2x

Two-point-two times as likely to be compromised if they sacrificed security

Mobile is helping governments and government agencies to serve their citizens and employees better, but it could also put sensitive data and critical systems in danger. 2019 saw a number of U.S. cities being held ransom by hackers, often causing disruption to important public services and infrastructure.

In fact, 77% of public sector organizations said that a mobile security compromise could put people's lives at risk. But public sector organizations are also worried about staff records being exposed – 90% said that their employees' data is as sensitive as that of the people they serve.

Yet despite the risks, 36% of public sector organizations had sacrificed security to "get the job done." And these organizations were 2.2 times as likely to have suffered a compromise – a bigger multiplier than in any other sector. Overall, 39% of public sector organizations had suffered a compromise involving a mobile device. That goes up to 44% for education organizations – a significant jump from our 2019 report.

enterprise.verizon.com/msi-public-sector

Back to table of contents >

Retail

30%

Thirty percent were compromised.

1.5x

One-point-five times as likely to be compromised if they sacrificed security

Retail, travel and hospitality companies are using mobile to appeal to modern consumers and keep physical stores relevant. Mobile is also helping to cut costs and waste from the supply chain. But there's also a lot at stake – 87% said they are concerned that a mobile security breach could have a lasting impact on their brand and customer loyalty.

Retailers are worried about a wide range of mobile security threats, from emerging ones like cryptojacking to more traditional threats like ransomware and phishing. But they're also concerned about "insider threats," rating their employees as the greatest risk when it comes to mobile devices.

Employee actions, even if inadvertent, can expose retailers to greater risk. 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 despite the risks, 40% of retailers had knowingly sacrificed mobile security. Our latest data shows that 30% had suffered a compromise – no improvement over our 2019 report.

enterprise.verizon.com/msi-retail

Small and medium-sized businesses

28%

Twenty-eight percent were compromised.

1.8x

One-point-eight times as likely to be compromised if they sacrificed security

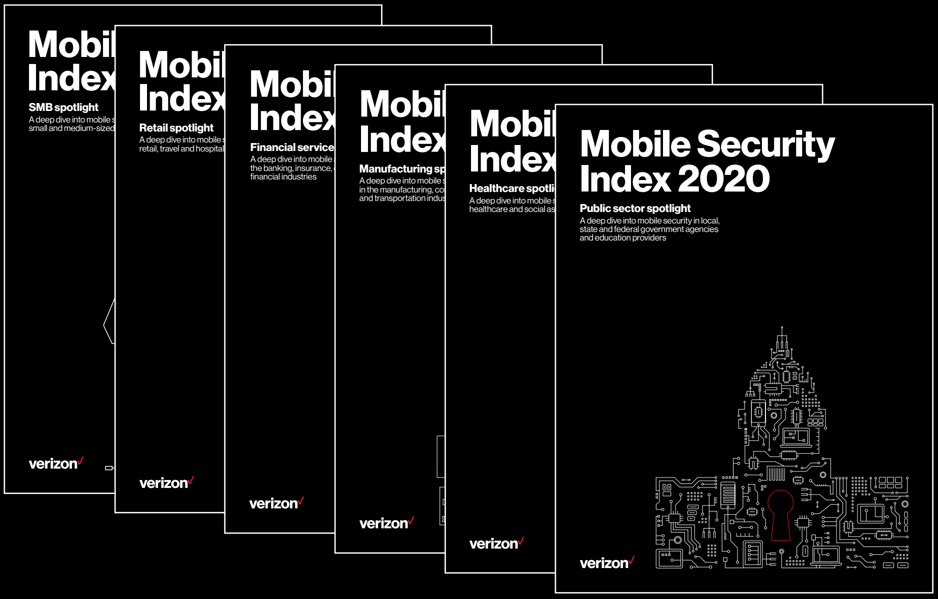
They might lack the resources and IT budgets of larger enterprises, but that's not holding small and medium-sized businesses (SMBs) back when it comes to innovation. Mobile and the cloud are levelling the playing field – 83% of SMBs said that cloud-based services are helping them to compete with larger businesses. And 80% said that using mobile to access business systems is key to their profitability and productivity.

But SMBs often lack the in-house expertise to react quickly and mitigate damage if hit by a mobile security compromise. As a result, the impact can be more severe and difficult to recover from – 43% said that mitigation was "difficult and expensive" compared to just 36% of larger companies. They can also find it harder to bounce back from the impact on their customers' confidence and order book. Over half (55%) said that they think that they have more to lose from a security compromise than a large enterprise.

Despite this, 39% of SMBs admitted to having knowingly sacrificed security. And while only 28% had suffered a mobile-related compromise, compared to 44% of larger companies, this is still a sizeable number and shows that hackers don't think SMBs are too small to care about.

enterprise.verizon.com/msi-smb

For a more in-depth look at the state of mobile security, take a look at our spotlights on SMBs; public-sector organizations; and the financial services, healthcare, manufacturing and retail industries.



Mobil
Index
SMB spotlight
A deep dive into mobile s
small and medium-sized

Mobil
Index
Retail spotlight
A deep dive into mobile s
retail, travel and hospital

Mobil
Index
Financial service
A deep dive into mobile
the banking, insurance,
financial industries

Mobil
Index
Manufacturing sp
A deep dive into mobile s
in the manufacturing, co
and transportation indus

Mobil
Index
Healthcare spotli
A deep dive into mobile s
healthcare and social as

Mobile Security
Index 2020
Public sector spotlight
A deep dive into mobile security in local, state and federal government agencies and education providers

verizon✓

Back to table of contents ›

3 Improving mobile security

It's important to start with getting the basics right—creating an acceptable use policy, using strong passwords, encrypting devices, training employees and securing cloud-based systems. But security isn't just about keeping attackers out and telling employees what they can't do. It's about empowering your people to do more, to innovate and to do their best work.

Back to table of contents >

Get the basics right.

Failing on basic security?

Many organizations still aren't doing enough to protect their mobile devices. Less than half (46%) said that they change all default/vendor-supplied passwords, and only 51% said they encrypt sensitive data when it's sent over public networks. Yet these are two of the most fundamental security precautions – along with regular security testing and restricting access to data on a "need to know" basis. Only 13% of companies had all four of these basic precautions in place. This isn't a one-off; it was 14% in our first report and 12% in last year's edition.

Worried about phishing?

Year after year, we see companies get hit by phishing attacks. Yet less than half of organizations (49%) in our survey said that they give their employees ongoing training on IT security. Having email protection in place is important, but it's not enough on its own. As we've mentioned, hackers are constantly innovating and finding ways to slip through these filters.

You can greatly improve your defenses by providing employees with ongoing training:

- Teach them how to recognize and report phishing, whether it comes via email, calls, apps or SMS
- Test their knowledge regularly
- Run mandatory retraining for those who score badly

Letting malware through?

Official app stores are constantly working to improve their scanning techniques and implementing more robust security filters, making them safer. However, many companies are letting employees roam the web and install whatever apps they choose, without such safeguards.

Despite the risks associated with malware and third-party apps, only 54% of organizations said that they restrict which apps their employees can install on mobile devices. And only 61% of organizations said they had a mobile device management (MDM), enterprise mobility management (EMM) or unified endpoint management (UEM) solution in place.

Ready to see how your mobile security stacks up to other organizations? This assessment tool can provide some powerful insights: enterprise.verizon.com/msi-assessment

> “
>
> **Across the board, criminal capabilities are outpacing most public and private spending in cybersecurity, as criminal profits are being reinvested into the development of new capabilities and an illicit black market for cyber tools and services.**
>
> —U.S. Secret Service[41]

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

Back to table of contents ›

Do you know where your data is going?

In a 24-hour period, a typical mobile device sends data to 10 countries via 18 apps.[42]

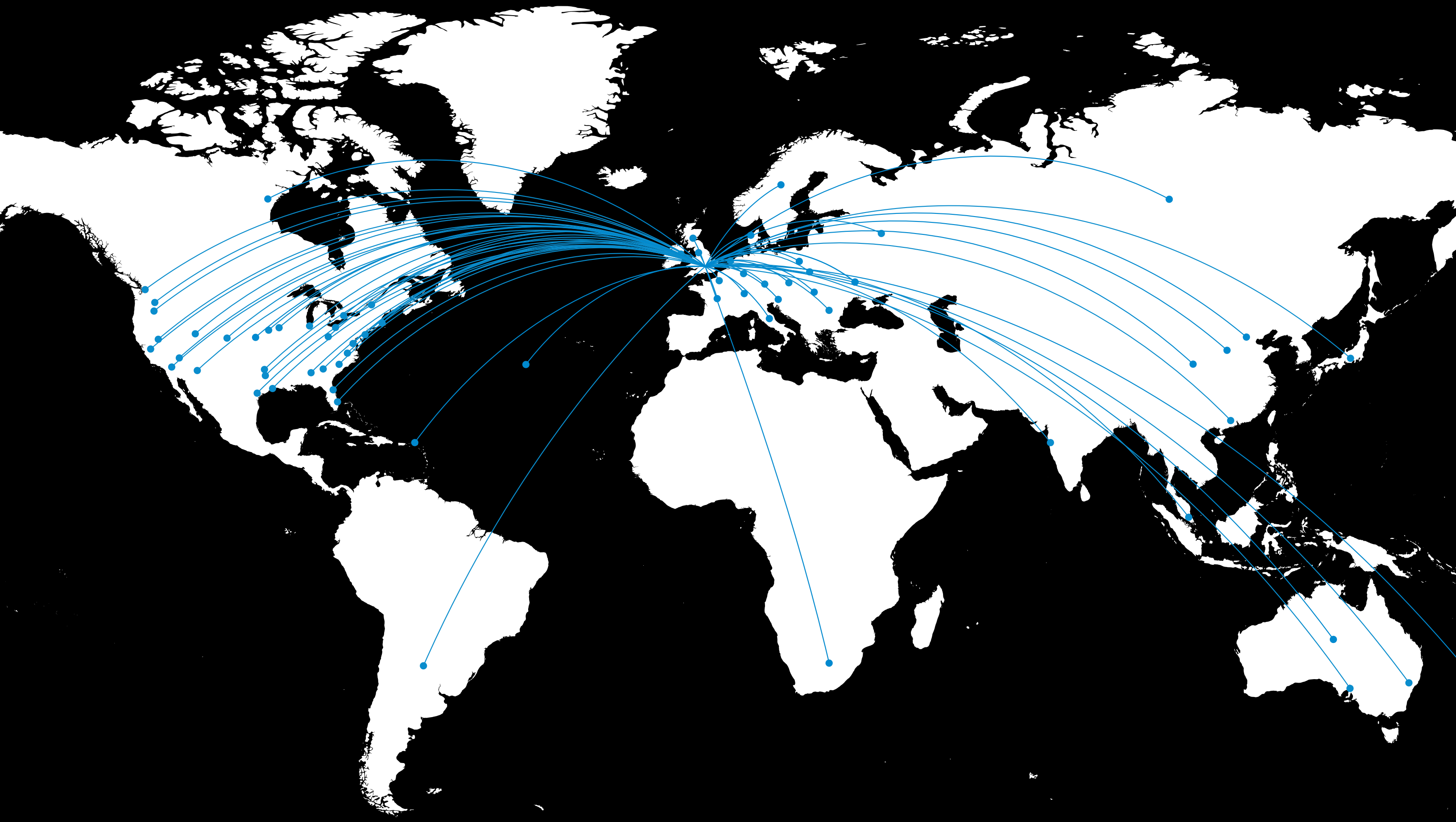
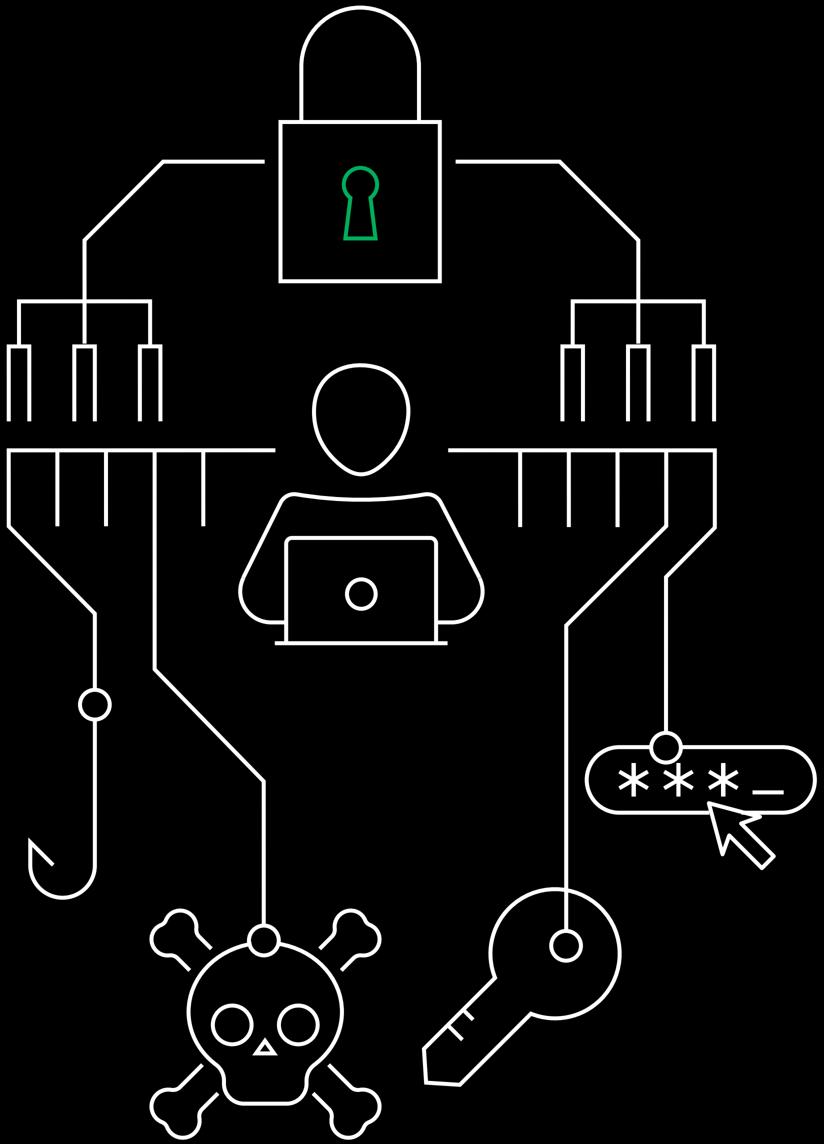


Figure 24. Data transfer from sample mobile user (with no known compromises) over 24-hour period, showing data being sent to 21 countries

Back to table of contents ›

Ask Donna.

Unit Chief Donna Gregory works for the Internet Crime Complaint Center (IC3), part of the FBI's Cyber Division. We asked her for advice on ways to help prevent some of the most common threats.



Q Donna, we found that just 13% of companies have four of the most basic security hygiene practices in place. What fundamental things do you think every company should make sure they are doing?

A It's important to patch the operating system, software and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through the use of a UEM, EMM or MDM tool and their patch management capabilities.

Additionally, mobile threat detection (MTD) solutions can offer anti-virus and anti-malware protection. Make sure that applications are set to automatically update and that scans are conducted regularly.

And it might be a cliché, but passwords, passwords, passwords. Despite all the evidence, many companies are still failing to ensure that all employees are setting strong passwords and keeping them secure. This makes life much easier for cybercriminals. Passwords should never be reused for more than one system and two-factor authentication should be enforced wherever possible.

But no matter how good your defenses are, there's always a risk of a compromise. Implementing physical and logical separation of networks and data for different organizational units can help limit the potential damage. Companies should implement least-privilege access for file, directory and network-share permissions.

Q How can companies reduce the impact of their devices being misplaced, lost or stolen?

A Missing devices are a fact of life. But every company should be using whole-disk encryption and PIN security codes on all of their devices. This means that even if it's stolen, the data on it will hopefully be rendered worthless to the attacker.

Q Ransomware remains one of the most prevalent threats. What can companies do to protect themselves?

A If you are infected, backups may be the best way to recover your critical data. But just installing a backup solution isn't enough. Companies should ensure that backups are not connected to the computers and networks they are backing up – for example, physically store them offline. It's also crucial to verify backups. A real-life emergency, when you need to restore data, is a bad time to find out that there's a problem.

Since end users are targeted, it's important that employees be made aware of the threat of ransomware and how it is delivered, and be trained on information security principles and techniques.

We'd also recommend implementing policies or other controls to prevent the execution of programs in locations commonly used by ransomware, such as temporary folders used by browsers and compression/decompression programs.

Q Phishing has been around for years, but attackers' techniques are getting much more sophisticated – especially when it comes to fraud, like business email compromise. How can companies keep their employees informed and vigilant?

A Training is obviously crucial. Teach your employees to check that an email address matches who it's meant to be coming from, especially when using a mobile or handheld device. They also should check that the URL is associated with the business it claims to be from, and watch out for hyperlinks that contain misspellings of the actual domain name. And as a rule, they should never supply login credentials or personally identifiable information (PII) in response to any emails.

There are also systems you can put in place to make it easier for your employees. For example, make sure the settings on their devices allow full email extensions and URLs to be viewed. And implement secondary channels or two-factor authentication to verify requests for changes in account information.

One simple thing you can do is configure your mail system to flag emails from outside your domain – many companies add a prefix, like [E], to the subject line. This makes it obvious when that email from the Managing Director is really from somebody masquerading as a colleague.

Q Malware is another classic threat that's getting increasingly sophisticated and harder to spot. How can organizations stay one step ahead of attackers?

A I've already said to install and maintain anti-malware software. But companies should also disable macro scripts from Office files transmitted via email. And they should consider using Office Viewer software to open Microsoft Office files sent via email. The functionality of these is limited – for example, macros don't work, compared to the full versions.

When it comes to avoiding malware-infected apps, it's true that sticking to official app stores isn't guaranteed to keep you safe, but it can greatly improve your odds. So we recommend restricting which apps users can install on their mobile devices and prohibiting those not from an official or company store.

Q Do you have any other advice to offer readers?

A Every organization should have a response plan in place and make sure that employees know how to report anything suspicious. This should be as easy to do as possible – employees are more likely to flag something if all they have to do is email security@yourcompany.com than if they have to log into an intranet, find a page and then fill out a form. Especially if they are using a mobile device.

And, forgive the self-promotion, but if there is a compromise, we'd encourage organizations to file a complaint at www.ic3.gov (or bec.ic3.gov for BEC victims) as soon as possible.

For additional insight from the FBI, see the Further Reading section on page 61.

Back to table of contents ›

Secure the mobile ecosystem.

Businesses are taking advantage of the opportunities offered by the cloud, and the number of powerful apps and solutions available is growing rapidly. But as the mobile ecosystem expands, it can introduce new risks to organizations.

Many of the things that businesses are using mobile devices for are enabled by the cloud. For most companies, it's now the default choice for building and running apps. In fact, 57% of companies said that over half the new business information they create or gather is stored in the cloud.

> **Mobile devices pose a unique set of threats to enterprises. Typical enterprise protections, such as isolated enterprise sandboxes and the ability to remotely wipe a device, may fail to fully mitigate the security challenges associated with these complex mobile information systems.**
>
> —National Institute of Standards and Technology (NIST)[44]

Are you staying on top of cloud-based apps?

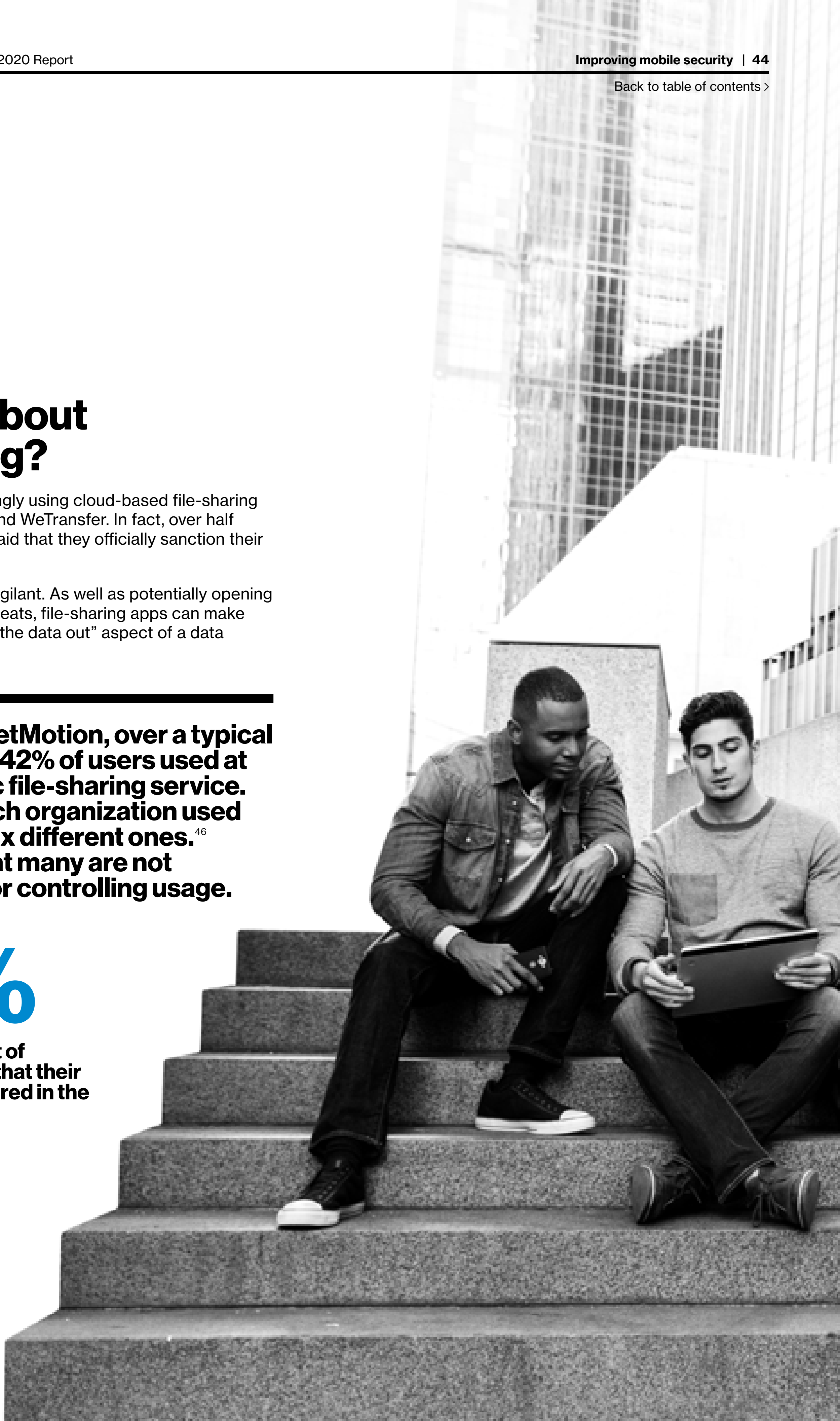
According to Netskope, cloud services—defined as requiring a login and being able to store and process data—now make up 85% of enterprise web traffic.[43] As well as the increasing use of cloud-based apps via mobile, this reflects the breadth of solutions in everyday use:

- Utilities open to all, often even without a subscription, like WeTransfer
- File storage, transfer and backup apps, like Dropbox, Egnyte and Box
- Publicly available tools used by consumers and businesses, like Slack and Trello
- Business productivity tools, like G Suite and Office 365
- Specialist tools managed through a web console and with web storage, like Adobe Creative Cloud
- Software-as-a-service (SaaS) apps aimed at businesses
- Corporate apps built in-house, often using third-party contractors

But most companies are massively underestimating just how many cloud-based apps their employees are using. Fifty-nine percent of companies said that their employees use no more than 250 SaaS/web-based apps. An analysis by Netskope showed that the average is actually much higher.

The average enterprise uses over 1,295 apps and cloud services, where more than 95% of these are unmanaged with no IT administration rights or even visibility. Of these, 96.3% are not "enterprise ready" and have a Netskope Cloud Confidence Index (CCI) of medium or less.[45]

Back to table of contents >



Worried about file sharing?

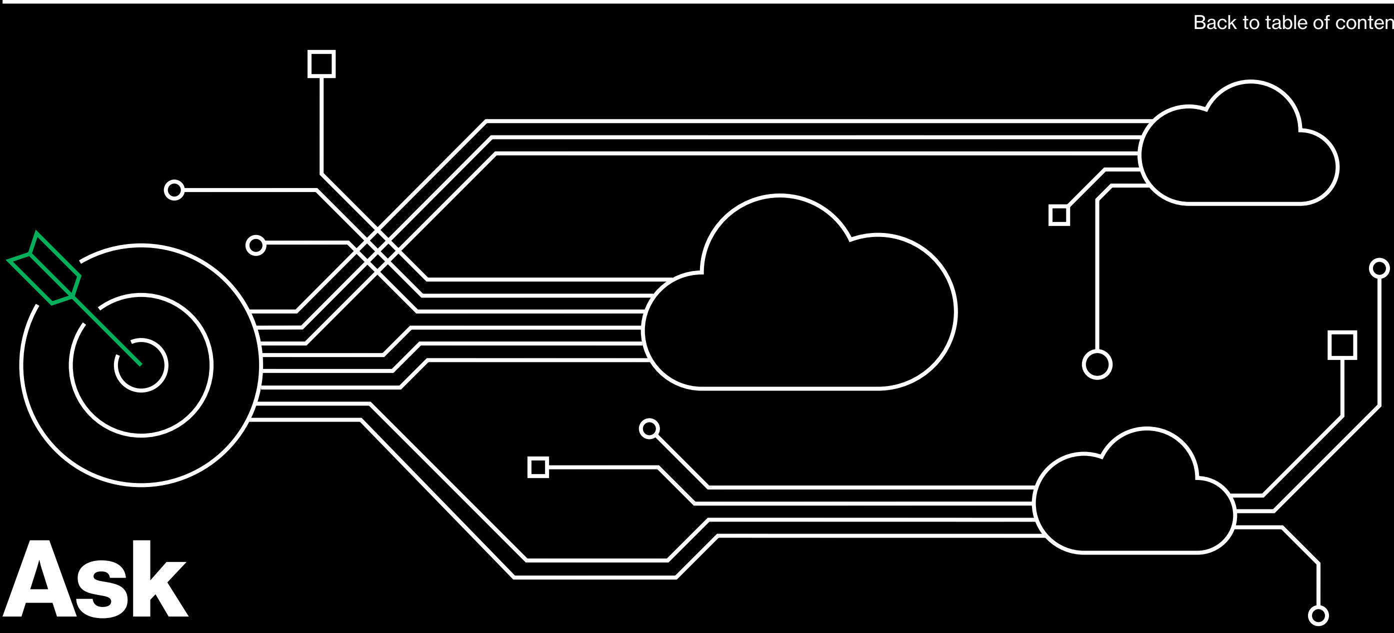
Enterprises are increasingly using cloud-based file-sharing apps such as Dropbox and WeTransfer. In fact, over half (55%) of organizations said that they officially sanction their use by employees.

Organizations must be vigilant. As well as potentially opening the door to additional threats, file-sharing apps can make exfiltration—the "getting the data out" aspect of a data breach—much easier.

According to NetMotion, over a typical 30-day period, 42% of users used at least one public file-sharing service. And in total, each organization used an average of six different ones.[46] This implies that many are not standardizing or controlling usage.

84%

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



Ask Gene.

Gene Stevens leads enterprise security product strategy for Verizon. He joined Verizon when it acquired ProtectWise, the network security company he cofounded.

Q Companies are ramping up their use of the cloud. What's the best way to do this without compromising on security?

A It was good to hear that most (83%) companies are taking specific measures to protect their cloud-based apps and services. But are they covering all the bases? Only about half (52%) said that they block the use of cloud apps when they're accessed from unknown networks, which is a basic precaution we'd like to see in all companies.

If you're sending data to third-party cloud services like Salesforce or Microsoft Office 365, I'd also recommend that you consider using a cloud application service broker (CASB). This can bolster your security by encrypting and tokenizing all of the data you upload to these services, and enforcing different levels of access based on the user's device, location and OS.

But a CASB alone will not give you all the visibility into a public cloud environment that you need. If you're deploying within the cloud, policy, configuration and access control are needed to enforce and track authentication and authorization. And yet, a visibility gap will still remain without an under-the-hood view into network traffic in public cloud environments.

To fill that gap, consider network detection and response technology that's run from the cloud and can perform full packet capture, deep packet analysis and security analytics to help detect threats. Detection and response is also effective for identifying threats at the endpoint, where user devices such as smartphones and laptops are connected.

Q With tens of thousands of web-based apps out there, how can companies vet those that their employees want to use?

A Just under half (44%) of companies said that they restrict the use of cloud apps to those with a proven security rating. While the number that are malicious is probably limited, many will have serious vulnerabilities. App rating services, like Netskope's Cloud Confidence Index, offer companies a degree of reassurance that the apps they're using meet their security requirements. They can help you understand your third-party risk, shortlist cloud services for adoption and identify compliance gaps so you can address them or arrange for compensating controls.

Q Many organizations are reliant on file-sharing apps. Others have banned them. Do you think they're worth the risk?

A Although useful, file-sharing apps can introduce new security risks. It can be difficult to regulate who employees are sharing files with, and to keep track of which recipients have access. If you want to play it safe, it's best to prohibit your employees from using file-sharing apps completely—18% of organizations have already done so.

Ultimately, all of this should be part of a larger strategy for securing your digital transformation. Beyond setting policies for cloud-based apps, you need to protect your own company's infrastructure. Security measures that are built into cloud services aren't enough. Tools that deliver pervasive visibility into your entire environment and enable rapid detection and response should be part of your plan.

Improve manageability and visibility.

The most advanced organizations are adopting a platform-based approach to mobile security. This means that security fades into the background, working invisibly but effectively. Instead of hindering your employees, it enables innovation and growth.

Need to deliver a better employee experience?

Putting the user experience first and creating well-designed security rules is important for your security posture. Badly designed or implemented security policies can be detrimental to both the user experience and company performance. Something as simple as a password policy could impede employees and increase support costs (due to more resets). And it's likely to drive up your cybersecurity risks, by frustrating your employees and driving them to circumvent the rules.

On the other hand, well-implemented security solutions can help 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. The best systems take a single-pane-of-glass approach and bring all of these solutions together, so you have better visibility of your users and defenses.

Want greater transparency and visibility?

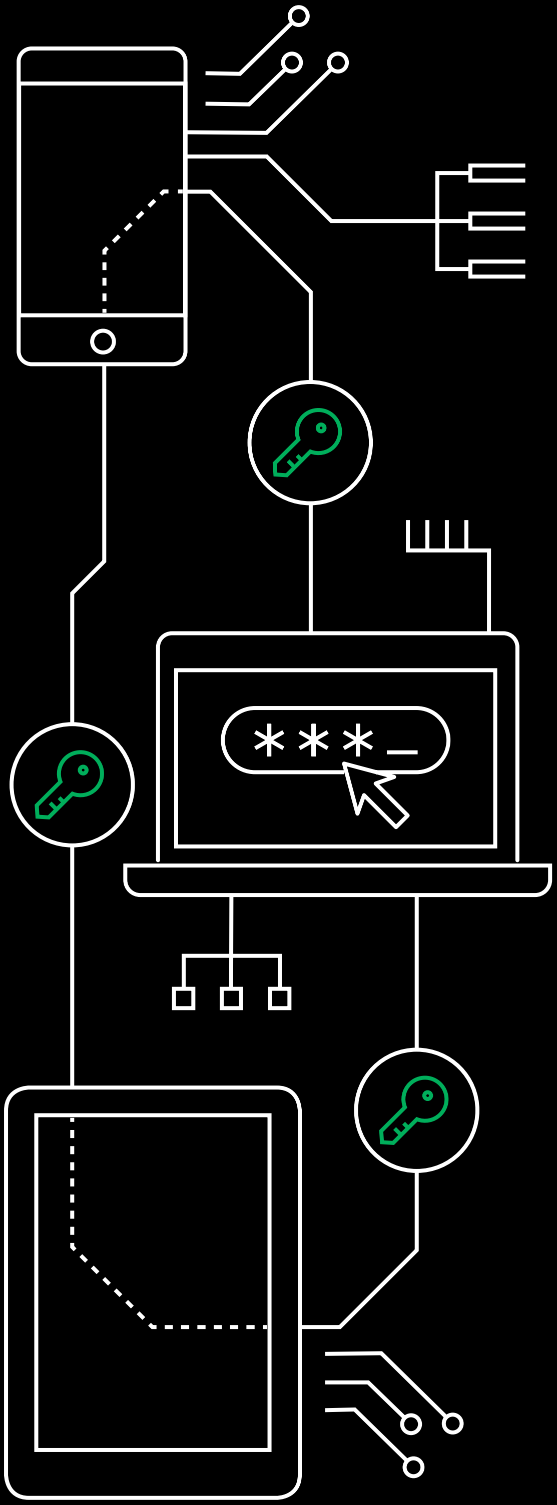
No matter how much you trust your employees, it's important to remember that humans are fallible. No amount of mobile training can guarantee that every staff member will follow the rules 100% of the time. They might be under enormous pressure to meet deadlines and decide to temporarily switch off their two-factor authentication (2FA). Or they might be stranded at an airport without mobile data–sometimes that's all it takes for someone to break a rule about using public Wi-Fi. That's why the best approach to security is one that has built-in controls that are automatically enforced, instead of relying on observance of policies. This can also help improve your transparency and visibility, as you don't have to rely on employees to report problems or behave in a certain way when nobody is watching.

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.[47]

> “
>
> **A set of security controls and countermeasures that address mobile threats in a holistic manner must be identified, necessitating a broader view of the entire mobile security ecosystem.**
>
> —NIST[48]

Back to table of contents ›

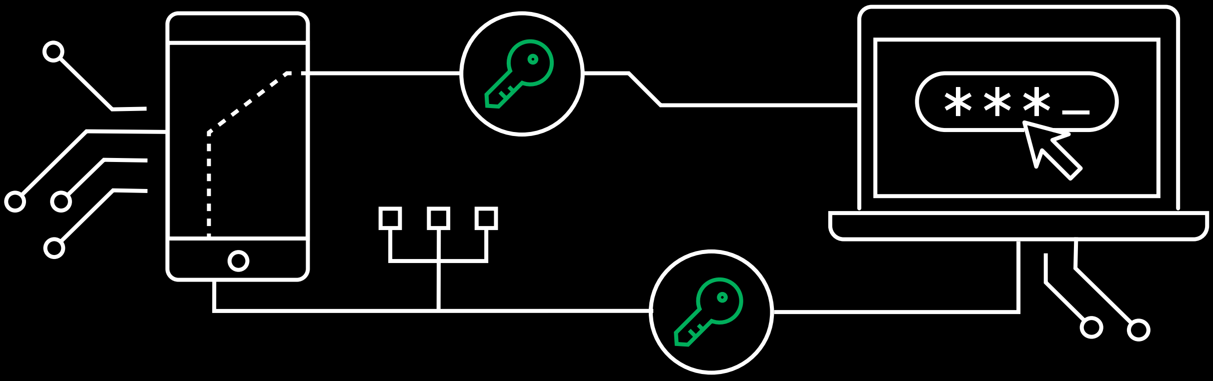


Ask Aspi.

Aspi Havewala is Director of Collaboration and Mobility at Verizon. He's responsible for messaging, collaboration and mobility services. We asked him about the best ways to secure mobile devices without negatively impacting the employee experience.

Q How would you recommend companies tackle improving their mobile device security, going from point solutions to an integrated and risk-based approach?

A You need to do some groundwork. This involves assessing the risks that are out there, the kind of company data you want to expose on the mobiles, what your stakeholders need and the preparedness of your employees. And once that's done, you can start to build a multilayered set of defenses. This means that if one layer fails, another layer kicks in and your devices, and your data and systems, are not left unprotected.



Q A lot of businesses are moving their applications to the cloud; does that make the job of people like you easier or harder?

A It comes with advantages and disadvantages. The disadvantage is, of course, it's out on the internet, anybody can access it. You can no longer protect that application in the traditional way you used to, which is behind the perimeter of a network, inside a company's firewall, isolating it on your own premises. But with all your data in a single place, you can direct all your energies toward securing that location, making sure that all of the controls are implemented around that one set of properties or that one application or that one cloud repository.

Q There's been a lot of talk lately about the "zero-trust" approach to mobile security, but what does it actually mean?

A Today's employees often depend on and work with contractors and visitors in the office. They may also be required to perform work tasks remotely. This means that trusting everyone inside a network can leave your organization vulnerable. Zero trust is based on the idea that you should implicitly trust no one – and instead look at a person's identity, access rights and device before granting them access to company data.

Just over a third (34%) of organizations said they're using a zero-trust policy.

Q Do you think zero trust is the right approach for organizations seeking to improve their mobile security?

A Most organizations have remote workers and assets stored in the cloud, so network perimeters are blurred. Adopting a zero-trust approach is an effective way of maintaining security when you have a distributed workforce – which is pretty much the norm now.

Zero trust can also help deliver better employee experiences. It's adaptive to each situation, so staff trying to do a low-risk task won't be impeded by superfluous security checks. That's because it doesn't just look at who is trying to gain access, but also at what they're trying to do. For example, an employee trying to sign into their email from home might encounter a standard level of authentication, say password and 2FA. By comparison, a user trying to set up a large bank transfer, accessing from a risky location or seeking to access privileged information could face more rigorous validation – this could include asking for biometric information – or be blocked.

Q Do you have any other advice for companies that want to improve their security without frustrating employees?

A First and foremost, prioritize the user experience. Make it part of every risk discussion you have, because a bad user experience is a big risk in and of itself. You should give your employees a range of options to do their work securely, and stay connected with your users. The more you communicate with them about the policy and controls that are in place, the more your users will appreciate security.

Next steps

Whether you're just starting a mobile security program or looking for ways to improve one, find the tools you need at enterprise.verizon.com/msi

- **Mobile security assessment tool** – See how your mobile security stacks up against 800+ businesses and get personalized recommendations for improvement
- **Acceptable use policy (AUP) guide** – An AUP is a foundational policy for mobile security. Our guide offers best practices for making your AUP stronger

Back to table of contents ›

4

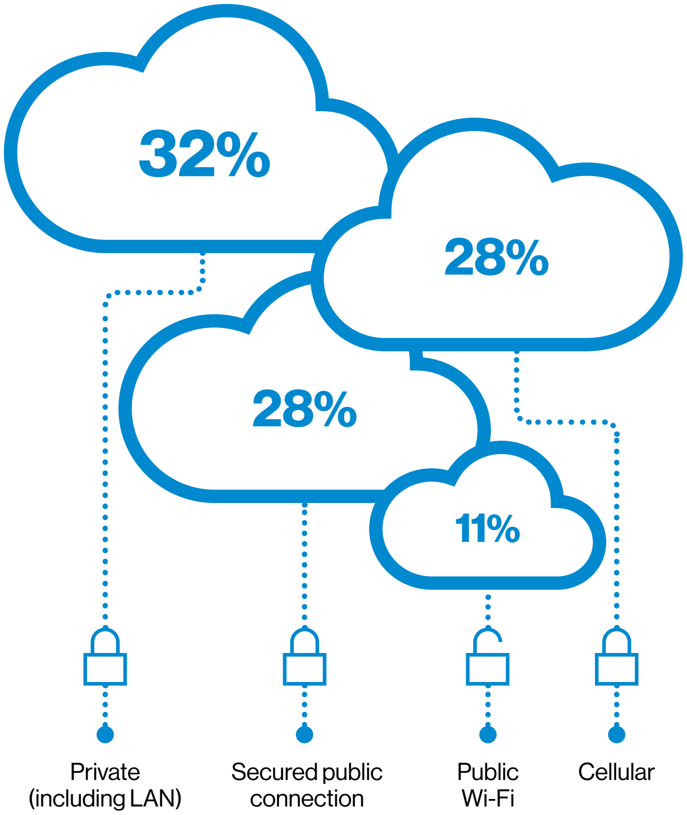
5G and IoT

5G is expected to play a crucial role in delivering the speed, security and connectivity required to support the next generation of mobile-driven disruption. And many Internet of Things (IoT) applications are built on mobile technologies. These technologies promise to transform almost every business sector, but this makes getting the security right even more important.

verizon✓

The opportunities and challenges of 5G

Data transfer to cloud-based apps



When people think of 5G, their first thought is often about speed. While it's true that dramatic improvements in speed are part of the equation, that's only one aspect of a much broader revolution.

5G opens up a whole new approach to managing and securing cellular networks. Wireless broadband for fixed locations will be one of the early use cases. This will help to enable higher bandwidth for areas with limited access and provide connectivity for events, pop-up stores and other temporary demands.

The anticipated speed and reliability of 5G means it may quickly become many businesses' first choice for data. 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.

5G is underpinned by a virtualized, cloud-based architecture that makes it easier to enable highly specialized functions—and security—for different network applications. In the future, this is expected to blur the distinctions between fixed networks (including those accessed over Wi-Fi) and cellular networks. Cellular already accounts for over a quarter (28%) of data transfer to cloud apps and, as 5G expands and more mobile tools are deployed to frontline workers, this number is likely to grow. In fact, 80% of our respondents said that within five years, mobile will be their primary means of accessing cloud services.

5G will transform many industries.

5G promises to deliver numerous benefits, including:

- **Increased productivity** – predictive maintenance of equipment, cutting downtime; more responsive supply chains; greater visibility of production
- **Enhanced customer experiences** – augmented reality in stores, personalization
- **Increased efficiency** – real-time monitoring of goods, cutting losses from spoilage and shrinkage; modelling of process changes using digital twins
- **Improved safety and well-being** – remote patient monitoring and telemedicine, improving patient care; smart safety monitoring, like collision avoidance systems – both on the road and in facilities like ports and warehouses
- **Increased automation** – autonomous vehicles, including delivery trucks; autonomous checkouts in retail stores

These are just some of the innovations that have been predicted or are being worked on. Few, if any, industries won't be affected.

Security features of 5G

As the number and variety of connected devices and applications grows, and the volume of data mushrooms, the "attack surface" will expand too. Fortunately, 5G has features to help counter that.

Better protection against unauthorized tracking and ID theft

When a device attempts to connect to a 5G network, it sends an ID in encrypted form. The Subscription Concealed Identifier (SUCI) is encrypted using the home network's public key. A private algorithm, the Subscription Identifier De-concealing Function (SIDF), enables the home network operator, and them alone, to convert this ID to the device's true identity, the Subscription Permanent Identifier (SUPI, akin to the IMSI in 4G).

This process helps prevent devices from being tracked or users' privacy being compromised. If the device has authenticated before, it may have been given a token (Globally Unique Temporary Identifier, or 5G-GUTI) that serves as a proxy for the SUCI. As tokens are short-lived, this helps to further conceal each device's identity. This is among the most significant security improvements in 5G over 4G.

Greater resilience against attacks

5G takes advantage of software-defined networking (SDN) and network function virtualization (NFV) technologies. One advantage of this move toward more network management being done in software is shorter update cycles. This will have numerous benefits, including enabling service providers to roll out new features more quickly and scale network functions more easily. As well as making networks more responsive to changes in traffic, this will mean that services can be independently isolated, restarted or replaced if they fall under attack.

Support for new devices and use cases

Less reliance on dedicated hardware means that service providers will be able to tailor security requirements to the specific needs of different use cases. For instance, highly sensitive applications, such as remote patient monitoring, could have the most rigorous and robust level of service, while a less sensitive application, such as weather monitoring, could operate with standard security and resilience. 5G also opens up new options for authentication to support a wider range of devices.

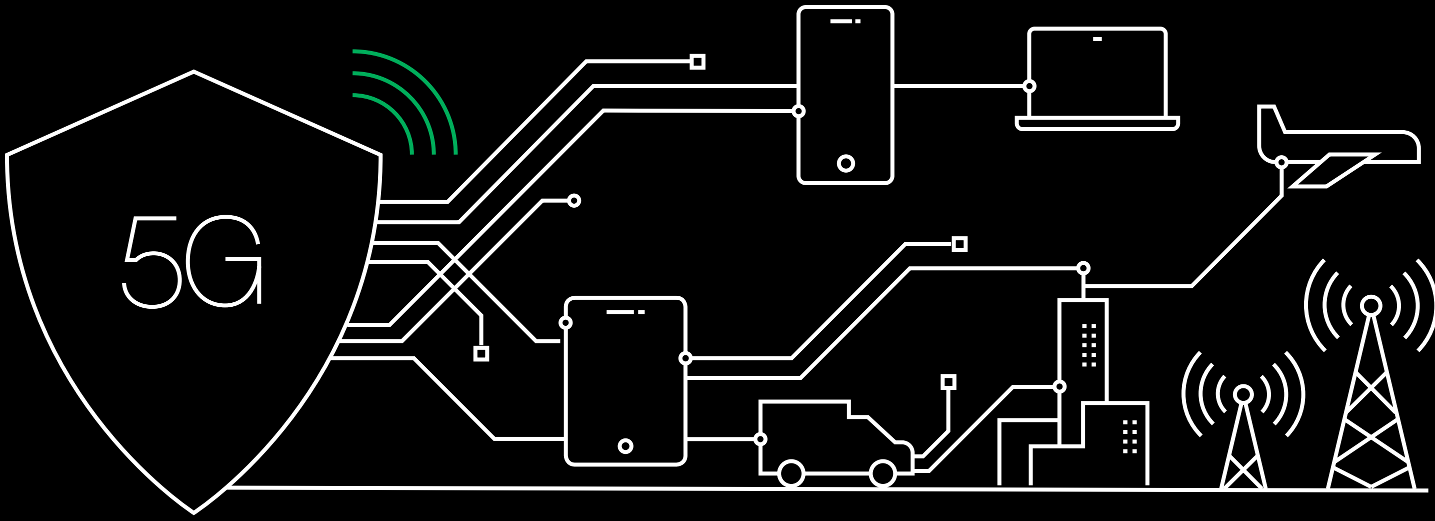
Improved protection when roaming

When a 5G device roams to a different network, typically when travelling abroad, the guest network may do some initial validation and refuse a connection if there is no roaming agreement, but that network must pass the user's credentials to the home network for final verification. This new procedure helps to prevent fraudulent attempts to obtain service or device credentials.

Better protection from rogue base stations

A rogue base station, also known as an "IMSI catcher" or "Stingray," imitates a legitimate cellular base station and enables criminals to commit MitM attacks, where they can eavesdrop on users' communications – both voice and data. When using a 5G network, as with 4G LTE, devices must authenticate the network using implicit keys derived from the key agreement procedure. 5G devices will also verify when using non-3GPP networks, such as Wi-Fi. This should help reduce MitM attacks.

Back to table of contents >



Ask Chandra.

Chandra McMahon is Verizon's Chief Information Security Officer. She is responsible for setting information security strategy, policy, standards, architecture and operations.

Q 5G sounds incredibly exciting, but isn't something new always a risk?

A Verizon was the first provider in the world to launch a commercial 5G service, but we would never have launched until we knew we were ready. Our reputation is too important to us for that.

While our 5G network provides a whole new experience for our customers, it's an evolution of our state-of-the-art 4G LTE technology. It leverages security measures that exist today in the 4G environment, but also ushers in new innovations such as sophisticated encryption and authentication features, as well as a new Security Edge Protection Proxy that helps prevent threats from less-secure interconnected networks from harming 5G networks.

Q But doesn't 5G increase the attack surface and introduce all kinds of new opportunities for cybercriminals?

A Verizon has a long history of protecting against threats to customers' security and maintaining the reliability and resilience of communications services against all manner of hazards, including cyberthreats. Our 5G network builds on our decades of experience and technological leadership.

We're deploying our 5G network with full awareness of the threats, and we are building it to account for them. This builds upon the innovations we've made in 4G LTE and leverages the unique benefits of 5G technology to develop and operate an even more secure network.

And our efforts aren't just limited to the technology itself. For example, as part of our 5G development, we've created detailed new vetting and compliance programs for vendors so we can be confident that every component we add to the network meets our exacting standards.

Back to table of contents ›

Q With so many new devices and types of applications, how can companies ensure that the latest exciting new thing doesn't compromise the security of their network?

A We use threat modeling to evaluate the potential risk of new applications and devices. Based on specifically identified threats, we conduct internal and third-party security testing on device and application layers to identify vulnerabilities that could be exploited, either by a nefarious internal actor or an external hacker.

This risk assessment determines whether any changes are required before we move forward with the product or service in question. We then work with the product or platform vendor to confirm that we have resolved identified issues prior to launch and that we have properly and securely configured the equipment and devices in question.

Q This is just the start for 5G, and as we've seen throughout this paper, as fast as operators and customers innovate, so do the attackers. How does Verizon plan to stay ahead of the threats and keep its network and its customers' data secure?

A Verizon actively participates in the standards development process to identify potential new security features that could be implemented in our network. And we plan to continue to lead the development of innovative security service concepts and capabilities for 5G. We're developing how we use AI, security automation, virtualization and other proactive security measures to accelerate the identification and mitigation of threats.

One of the most interesting things that we're working on is using a software-defined perimeter (SDP) to create a "zero-trust" security layer over a 5G network. This offers big benefits for customers with complex networks and security needs.

Finally, we're investing in our people too. From talent recruitment to career development, we're investing in building a robust cybersecurity workforce pipeline to ensure our customers' needs are met today and tomorrow.

Securing the IoT

Back in 2015, some experts predicted that there would be more than 50 billion connected devices by 2020. The forecasts are now more modest—according to Ericsson, there were nearly 11 billion connected devices at the end of 2019, and that will rise to nearly 25 billion by the end of 2025[49]—but the hype has been replaced by results. When asked how critical Internet of Things (IoT) devices are to the smooth running of their organization, 65% of respondents answered eight or more on a 1–10 scale.

Adopters are using IoT for a wide range of purposes. Most commonly, they are using it to monitor the efficiency of equipment, enhance productivity and monitor the physical security of buildings (all over 60%), and to enhance products and services for customers (48%). Just over a quarter (26%) are using it to measure the wellness of people.

IoT devices are having a major impact in nearly every sector. The volume and variety of devices using wireless connectivity has grown massively. Two-thirds of respondents are using cellular networks to connect their IoT devices.

IoT is no longer in its infancy. Almost half (49%) of those that we surveyed that were using IoT had at least one full-scale deployment. And a third (33%) said they have over 1,000 IoT devices in use. That goes up to two-thirds (67%) in retail, where IoT-based technologies are enabling frontline staff to deliver better customer experiences and providing insight that's helping to manage inventory and keep physical stores relevant.

The survey results in this section are based on respondents responsible for buying, managing and securing IoT devices, such as connected wearables, smart building equipment and fleet management systems.

How critical is IoT to the smooth running of your business?

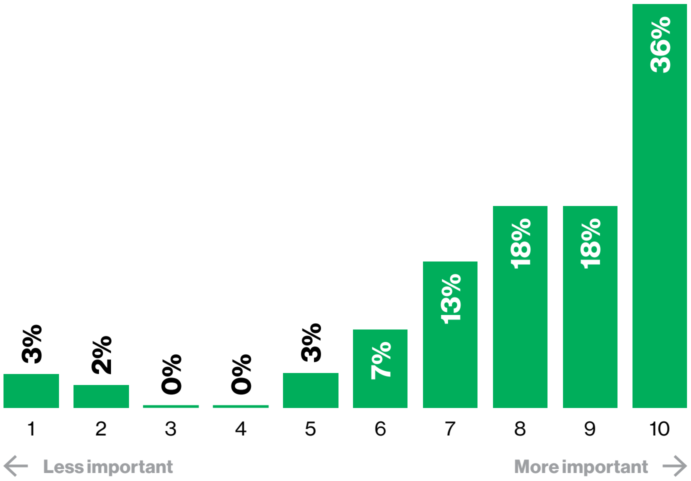


Figure 25. On a scale of 1 to 10 (very), how important are your IoT projects to the smooth running of your businesses (those with fully deployed IoT projects)?

Which categories do your IoT projects fall into?

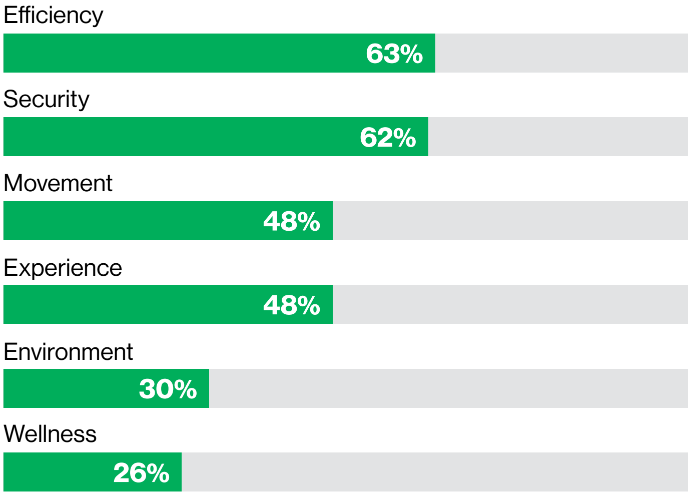


Figure 26. Which of the following categories do your IoT projects fall into?

Back to table of contents ›

> “
>
> **Cybercriminals are using IoT proxy servers to provide a layer of anonymity to mask their attacks on other devices. Devices in developed nations are particularly attractive targets as they can facilitate access to systems that block traffic from suspicious or foreign IP addresses.**
>
> —FBI[50]

What new risks does IoT introduce?

The use of IoT brings its own challenges. Since devices are often in remote locations, they can be vulnerable to physical tampering or network attack. Seventy-six percent of IoT respondents said that at least some of their devices are difficult to access, either embedded in a system or in a remote location, making them harder to update or replace.

It’s important to look ahead when designing devices – over a third (36%) of companies said that the anticipated lifetime of their IoT devices is five years or more – but you can’t plan for everything. Many early devices lack security features that are now critical and lack the ability to update software and firmware remotely.

It’s not just the actual data being captured by IoT devices that’s at risk. Over a quarter (26%) of IoT respondents think that their devices are of less interest to hackers than other systems – but it’s possible that they’re unaware of how easily IoT can be used as a gateway into their network. A cybercriminal could use IoT devices as a stepping stone to more sensitive data and wider business systems. A well-known example involved a hacker getting into a smart HVAC system maintained by a third party and using this as a lever to steal the details of millions of payment cards from a major retailer.

New and emerging threats

The sheer volume of IoT devices, many with weak security protection, presents a huge opportunity for hackers. That connected doorbell might improve your home’s or office’s physical security, but it could also be a Trojan horse for your IT security. Many IoT products have been found to have extremely weak cybersecurity – including, worryingly, devices such as smart locks. A single vulnerable IoT device could offer hackers a virtual open door to your network and everything that’s attached to it.

Many hackers are also looking to exploit the lack of visibility many users have into what their IoT devices are doing. They are planting malware on the device to create a botnet – an army of devices typically used for things like distributed denial-of-service (DDoS) attacks. The device continues to work as normal, so the owner is completely unaware of its side hustle. In 2019, a botnet used more than 400,000 IoT devices to launch an attack, similar to the Mirai botnet that wreaked havoc in 2016.

Data tampering is another significant threat. This occurs when hackers modify data in transit. This can have serious consequences in industrial or manufacturing environments. For example, inaccurate or falsified data transmitted from heat or temperature sensors could not only ruin batch production, it could destroy equipment or endanger employee safety.

When deploying IoT devices, you should also be wary of SIM theft. This is attractive to attackers because of the low effort required – often all they need is a screwdriver. The hacker physically breaks open a connected device, such as a smart lamppost, and removes the SIM card. They then put the SIM in their own device, and take advantage of free calls and data at the company’s expense.

Almost one in three were hit.

Stories about connected cars being susceptible to hacking might make better news than a HVAC system actually being compromised, but that’s masking the real danger. Nearly a third (31%) of IoT respondents admitted to having suffered a compromise involving an IoT device. That goes up to 52% for information and media companies, and 47% for retail. The public sector was least likely to be hit, but still almost a quarter (23%) were compromised.

Cutting corners is partially to blame. Two-fifths (41%) admitted to having sacrificed IoT security to “get the job done.” As with mobile device security, 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.

Mirai is open source malware code that turns networked devices into bots. It has been behind some of the largest and most DDoS attacks ever reported—over 1 Tbps. It primarily targets connected consumer devices, such as home routers and surveillance cameras.

Back to table of contents ›

Data privacy matters.

But it is still a work in progress for many of the organizations using IoT.

78% **Seventy-eight percent of IoT respondents think that data privacy will be a key brand differentiator in the future.**

84% **Eighty-four percent said that they gather personally identifiable information (PII) using their IoT devices, and 25% of those don't even anonymize it.**

The use of encryption is growing.

The vast majority of the companies we interviewed thought that their IoT data was of value to hackers. Despite this, less than half (47%) said that they encrypt all IoT data sent across public networks.

The major cloud service providers (including Amazon Web Services, Microsoft Azure and Google Cloud Platform) are enforcing best-practice security policies, such as encrypting all message queuing telemetry transport (MQTT) traffic—a lightweight protocol used for IoT data. According to Asavie, the volume of MQTT traffic that is encrypted is up from 55% 12 months ago to 65% in its latest data. Hopefully this indicates that more companies are now aware of the need to apply encryption to their IoT traffic.[51]

Why are companies cutting corners?

Seventy-six percent of respondents said their organization is at moderate to significant risk from IoT device threats. So why are they sacrificing security? The top reason given was expediency—60% said that time pressure was behind the decision. In the drive to get to market quickly, security often takes a back seat. Over half (51%) said that security is not a priority for v1.0 (minimum viable product); it's something they "can worry about later."

Another reason behind many security shortcuts is design restraints. IoT devices tend to be small and compact, and not all of them are very "smart." When designing IoT products, it's often tempting to bypass the security features that are standard for more sophisticated mobile devices.

Value of IoT data to hackers

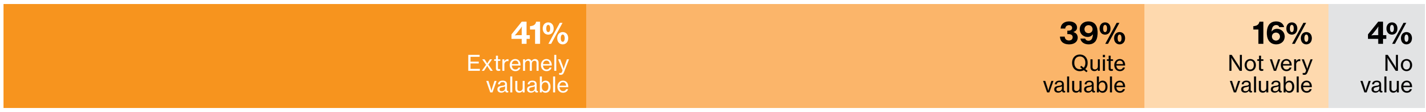


Figure 27. How valuable is the information that you gather via IoT sensors to hackers?

Back to table of contents >

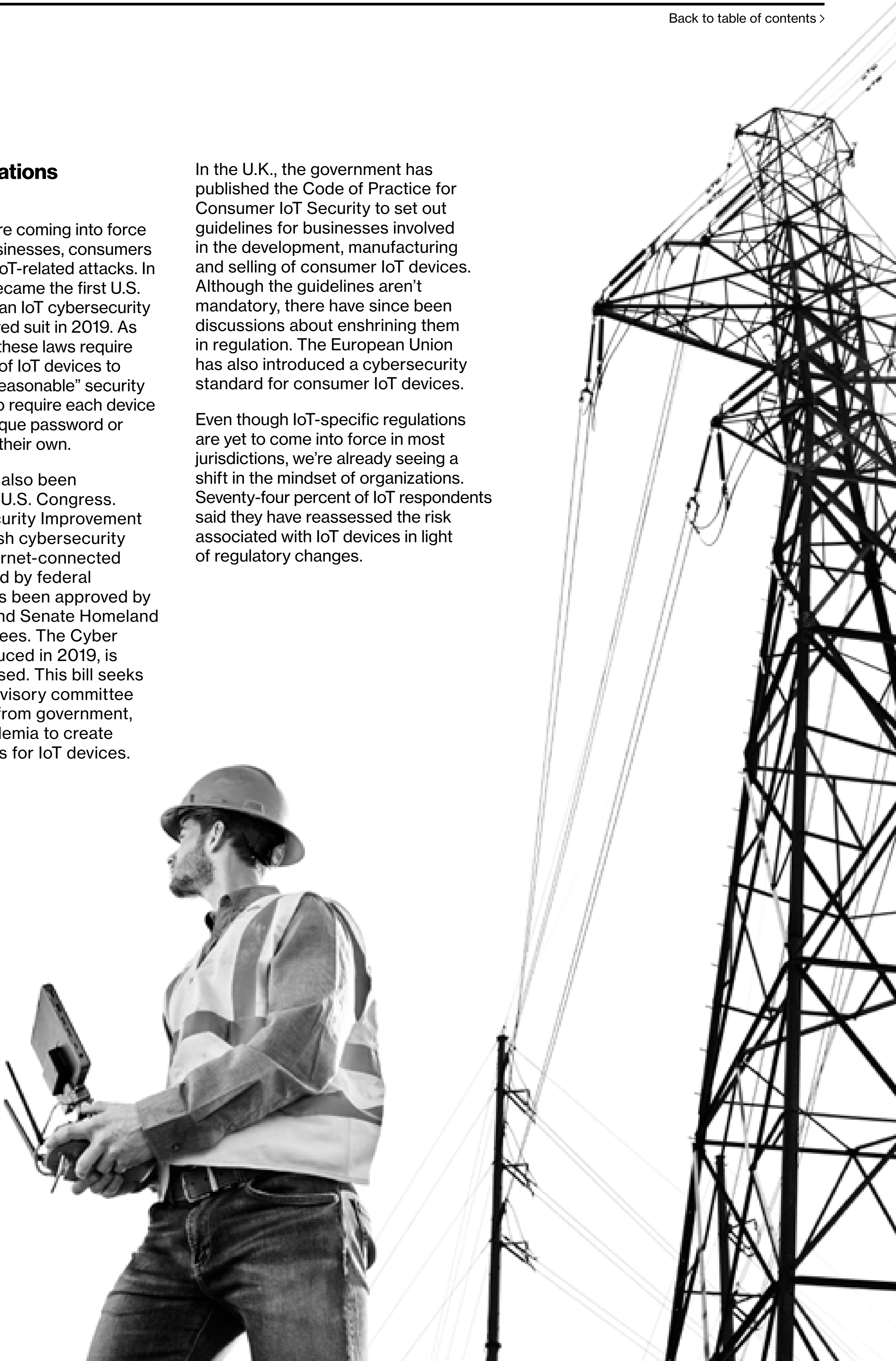
Will new regulations drive change?

New regulations are coming into force to help protect businesses, consumers and citizens from IoT-related attacks. In 2018, California became the first U.S. state to introduce an IoT cybersecurity law. Oregon followed suit in 2019. As of January 2020, these laws require any manufacturer of IoT devices to equip them with "reasonable" security features. They also require each device to come with a unique password or force users to set their own.

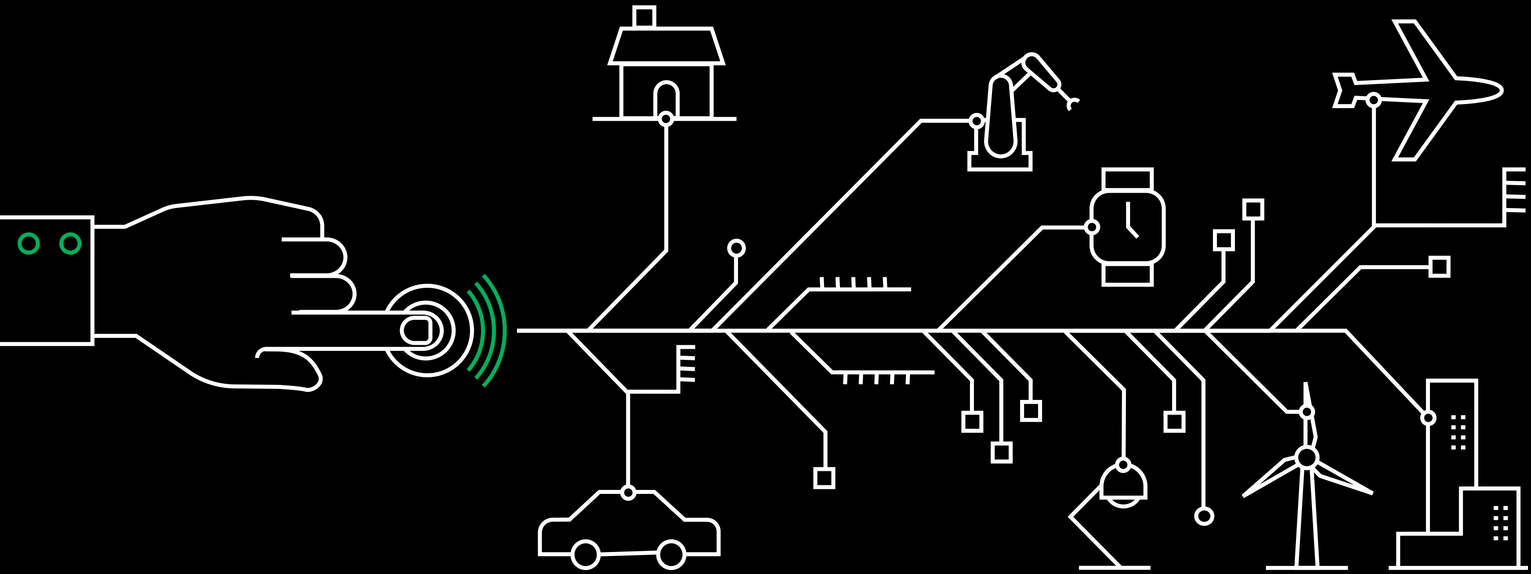
Several bills have also been introduced to the U.S. Congress. The IoT Cybersecurity Improvement Act would establish cybersecurity standards for internet-connected devices purchased by federal agencies. This has been approved by both the House and Senate Homeland Security Committees. The Cyber Shield Act, introduced in 2019, is also being discussed. This bill seeks to establish an advisory committee of cyber experts from government, industry and academia to create cyber benchmarks for IoT devices.

In the U.K., the government has published the Code of Practice for Consumer IoT Security to set out guidelines for businesses involved in the development, manufacturing and selling of consumer IoT devices. Although the guidelines aren't mandatory, there have since been discussions about enshrining them in regulation. The European Union has also introduced a cybersecurity standard for consumer IoT devices.

Even though IoT-specific regulations are yet to come into force in most jurisdictions, we're already seeing a shift in the mindset of organizations. Seventy-four percent of IoT respondents said they have reassessed the risk associated with IoT devices in light of regulatory changes.



Back to table of contents >



Ask Steve.

Steve Szabo is Head of Global Products and Solutions for Verizon's Internet of Things (IoT) business unit. He's responsible for delivering industry-leading solutions leveraging Verizon's 4G LTE, NB-IoT and CAT-M1 networks. His current focus is producing next-gen solutions powered by 5G and mobile edge computing. We asked him about the state of IoT security.

Q Steve, we've heard a lot of talk recently about SIM theft–people literally breaking into smart devices and stealing SIMs. What's the best way for organizations to defend themselves against this?

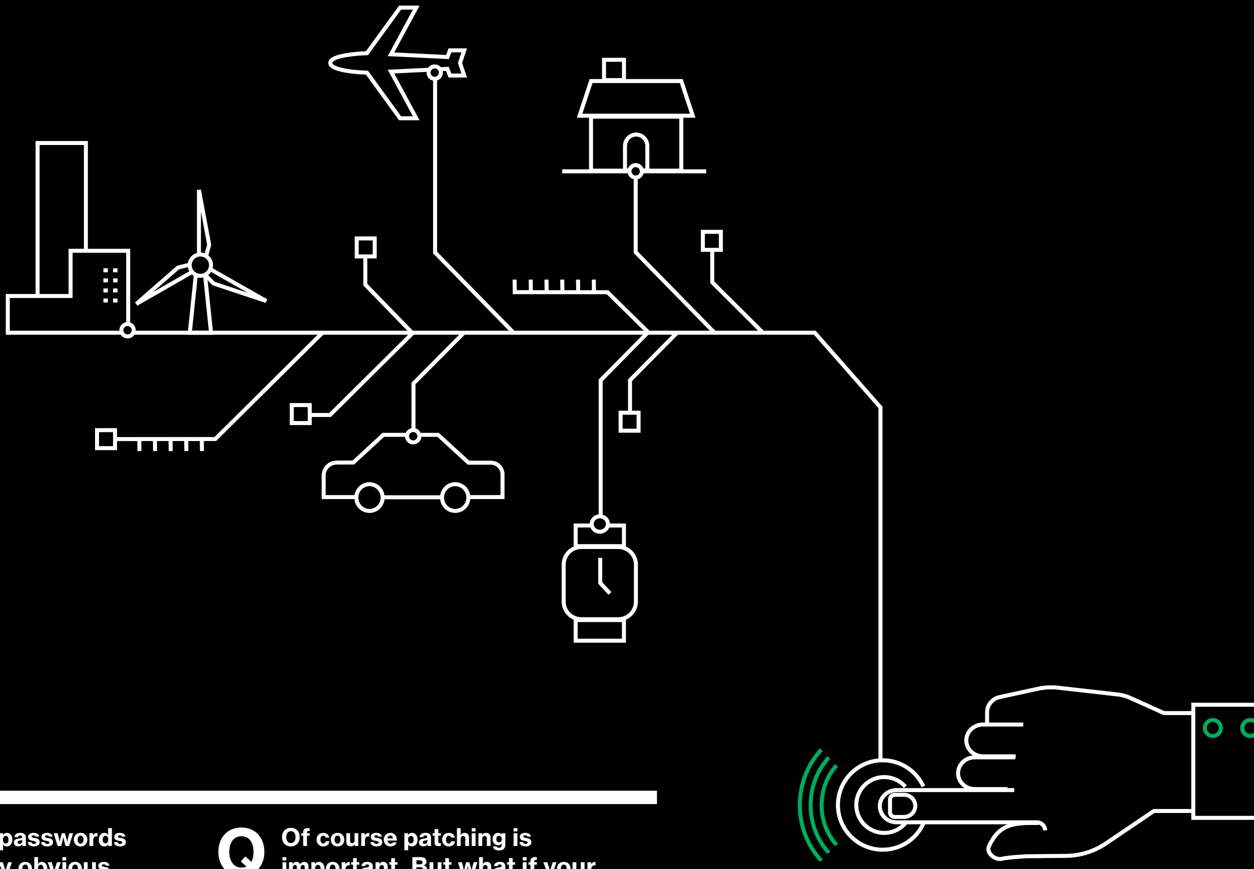
A The level of risk really depends on where your devices are located. But whatever the case, your best defense is binding each SIM card to the device via its IMEI. This means the attacker can't use the SIM by simply putting it into another device. An IoT platform should enable you to set a data limit per device–so even if a criminal gets their hands on the SIM, their spending, and your losses, will be capped.

Q Is it realistic to expect companies to encrypt all of their IoT data? What about really basic sensors that are only transmitting something simple like a temperature reading?

A Encryption is a powerful tool, but isn't used nearly as often as we'd like to see–despite the availability of new chips designed for the size, power and price constraints of IoT devices.

We recommend encryption for all applications and networks, for data at rest and in transit. Even data as seemingly innocuous as temperature readings might be of value to a hacker–for example, does it include when a building is in use and when it's not? Also, what if a criminal were to intercept communications and feed incorrect readings into the system? This could increase energy bills or cause harm to temperature-sensitive products like food and medicine.

Back to table of contents >



Q Changing default passwords seems like a pretty obvious precaution to take. Why are so many people and companies still failing to do it?

A I think there's still a lot of naivete when it comes to IoT risks. A lot of people think it's just the data held on their devices that's at risk. But by hacking that device, an attacker could use it as a foothold to gain access to so much more. Of course, expediency is also likely to be a factor. Having unique passwords for hundreds of devices requires processes, and there's often pressure to deliver quickly—as our survey shows.

Q Of course patching is important. But what if your devices are in remote locations or buried many feet underground?

A Lots of organizations have IoT devices in locations really difficult to access. But it's not just location that makes many IoT devices difficult to update; many IoT devices are built to be as small as possible and as frugal as possible—36% of IoT respondents said that they expected devices to last over five years. That's a lot if you're using a battery.

Despite these constraints, we think that it's critical to build in the functionality to perform updates securely over the air (OTA). OTA updates enable you to patch any vulnerabilities and take advantage of new security practices as they emerge. It also gives you more opportunities to improve functionality over the device's lifespan.

Back to table of contents ›

5

Appendices

Want to learn more about this report, mobile security or the broader cyberthreat landscape? In this section, you'll find information on our survey methodology, details about the data referenced in this report, bios of our contributors and recommended further reading—from law enforcement advisories to spotlights on specific industries and segments.

verizon✓

Back to table of contents >

Further reading

Verizon thought leadership

Verizon is committed to sharing analysis and insights with the rest of the industry, law enforcement, and public- and private-sector organizations in the interests of improving the security of devices, data and critical infrastructure. As part of this commitment, we publish a number of pieces of research and thought leadership.

Other Verizon Mobile Security Index publications

Industry spotlights

These concise reports provide detailed insights into the state of mobile security in four key vertical sectors: finance, healthcare, manufacturing and retail.

Financial services: enterprise.verizon.com/msi-financial-services

Healthcare: enterprise.verizon.com/msi-healthcare

Retail: enterprise.verizon.com/msi-retail

Manufacturing: enterprise.verizon.com/msi-manufacturing

Small and medium-sized business spotlight

This report gives a deep dive into the threats companies with up to 499 employees are facing.

enterprise.verizon.com/msi-smb

Public sector spotlight

Learn about the state of mobile security in the public sector—including local, state and federal government and educational institutions.

enterprise.verizon.com/msi-public-sector

Other Verizon security reports

Data Breach Investigations Report

The DBIR is one of the IT industry's foremost security publications. Since 2008, it has provided highly respected insight into the state of cybersecurity based on analysis of real incidents. Overall, the DBIR team has analyzed over 375,000 security incidents, including nearly 18,000 confirmed data breaches, from around the world. The 13th edition will be published in early 2020.

enterprise.verizon.com/DBIR2019

Insider Threat Report

The Insider Threat Report provides detailed insights on five main causes of internal data breaches, so you can strengthen your cybersecurity protections and reduce the risk of valuable assets being compromised from within your business.

enterprise.verizon.com/2019-insider-threat-report

Payment Security Report

Verizon's annual Payment Security Report on payment card security has become vital reading for those responsible for security payment systems. Driven by its analysis of compliance with the Payment Card Industry Data Security Standard (PCI DSS), it offers valuable insight into building proactive, robust security controls and achieving genuine data protection, not just passing the test.

enterprise.verizon.com/2019-psr

Back to table of contents ›

Data Breach Digest: Telephonic pretexting, identity theft and Wi-Fi compromise

Insights into common cyberattack scenarios, based on real incidents investigated by the Verizon investigative response team.

Pretexting: enterprise.verizon.com/resources/casestudies/data-breach-digest-2018-the-double-fake.pdf

Identity theft: enterprise.verizon.com/resources/casestudies/data-breach-digest-2018-the-achilles-steal.pdf

Evil twin: enterprise.verizon.com/resources/casestudies/data-breach-digest-2018-the-evil-twin.pdf

Additional resources from government and law enforcement agencies

FBI advisory on business email compromise

Read the FBI's statistics on the rise of reported incidents of BEC/EAC fraud around the world, and total reported losses. And learn how to protect your own organization.

ic3.gov/media/2019/190910.aspx

FBI advisory on ransomware

Find out how cybercriminals use a variety of techniques to infect their victims' systems with ransomware, how you can protect your organization and what you should do if you've been affected.

ic3.gov/media/2019/191002.aspx

Mobile security updates from NIST's center of excellence

The National Cybersecurity Center of Excellence (NCCoE) mobile device security efforts are dedicated to solving businesses' most pressing mobile cybersecurity challenges.

nccoe.nist.gov/projects/building-blocks/mobile-device-security

NIST guidance on corporate-owned personally enabled (COPE) devices

Helpful guidance on managing COPE mobile devices and reducing the risk these devices can pose to cybersecurity.

nccoe.nist.gov/sites/default/files/library/sp1800/mdse-nist-sp1800-21-draft.pdf

U.K. Home Office buyers' guide to mobile security

Simple guidance on securing your mobile device from the Home Office of Her Majesty's Government of the United Kingdom, responsible for immigration, security, and law and order. Suitable for sharing with device users.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/510735/Mobile_device_security_leaflet_240316_web.pdf

Back to table of contents ›

Methodology

We contracted an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices. Respondents were invited to complete one of two surveys, one on mobile devices (including tablets, laptops enabled with cellular or Wi-Fi connectivity, and mobile phones) and one on IoT devices (such as connected wearables, smart building systems and fleet management systems).

In total, 876 professionals responsible for the buying, managing and security of these devices responded. The following charts break down the demographics of these respondents.

Our sample included both small companies and large enterprises. Company size was not a strong indicator for most of our questions. Unless stated otherwise, all data in this report is from these surveys.

Mobile respondents

Respondents by industry

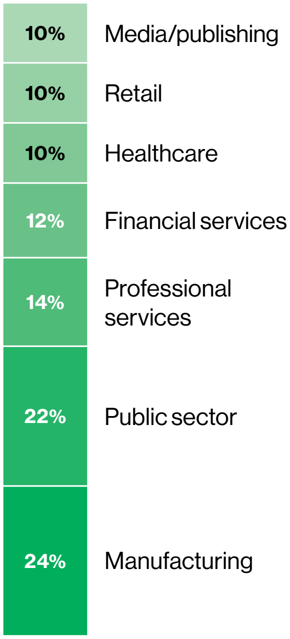


Figure 28. Number of respondents by industry

Respondents by number of employees

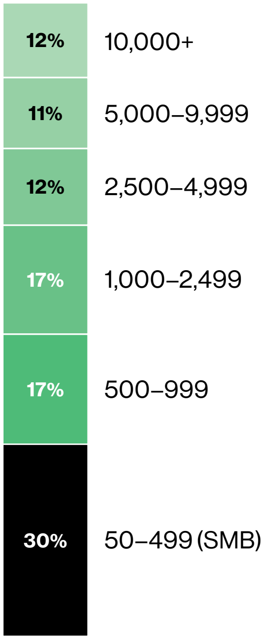


Figure 29. Number of respondents by company size

Respondents by role

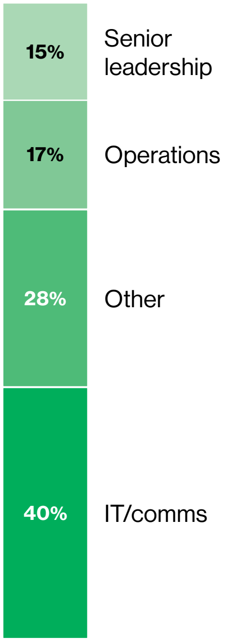


Figure 30. Number of respondents by department/role

IoT respondents

Respondents by industry

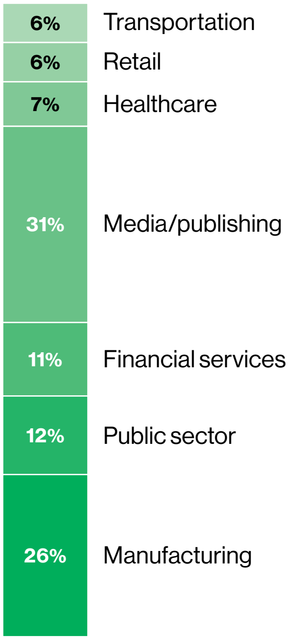


Figure 31. Number of respondents by industry

Back to table of contents ›

Contributors

Security companies

Asavie

Asavie simplifies digital transformation for enterprises and OEMs, including the most advanced IoT and enterprise software-defined wide area network (SD-WAN) deployments. Its self-serve, programmable SaaS solutions enable secure mobile access in a multicloud, multinetwork world. It unifies visibility and control across all of an organization's mobile and IoT endpoints, as well as legacy greenfield implementations, providing intelligent insights to help reduce costs and improve overall performance. It is an ISO27001 certified company.

Information supplied by Asavie for this report is based on anonymized data gathered from its base of more than 10,000 enterprise customers over the first nine months of 2019.

asavie.com

IBM

IBM Security MaaS360 is a UEM solution that uses AI and analytics to transform the way organizations support users, apps, content and data across every type of device. Its open, cloud-based platform integrates with preferred security and productivity tools, allowing modern businesses to derive value quickly.

The MaaS360 Mobile Metrics feature offers cloud-sourced benchmarking data and best practices to enhance productivity and improve security. Benchmarking data is generated by leveraging multiple data values from MaaS360 client implementations to build aggregated metrics.

ibm.com/security/mobile/maas360

Lookout

Lookout is a cybersecurity company for the post-perimeter, cloud-first, mobile-first world. It is trusted by hundreds of millions of individual users, enterprises and government agencies, and partners such as Verizon, Microsoft and Apple. Powered by the largest data set of mobile code in existence, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk. The installed base of Lookout's personal and enterprise mobile endpoint products is over 170 million mobile devices worldwide. This acts as a global sensor network that provides visibility into the threat landscape, including over 70 million apps—and that's growing by up to 90,000 apps a day.

Lookout leveraged its mobile data set to provide data used in this report. It also helped analyze the results and provided insight on the current threat landscape.

lookout.com

MobileIron

MobileIron's mobile-centric, zero-trust approach is built on a UEM foundation to secure access across the perimeter-less enterprise. Its approach to security helps to reduce risk by giving organizations complete control over their business data as it flows across devices, apps, networks and cloud services. MobileIron UEM puts enterprise mobile security at the center of your enterprise and allows you to build upon it with enabling technologies such as zero sign-on user and device authentication, multifactor authentication and mobile threat detection.

Unless otherwise specified, MobileIron data points given in this report are based on aggregated usage data from devices with threat detection activated across the installed base of MobileIron Threat Defense and Zimperium, gathered over the course of 2019.

mobileiron.com

Back to table of contents ›

NetMotion

NetMotion offers an intelligent software solution for today's modern, mobile organizations. This enhances connectivity and security for users while providing complete visibility and control for IT teams with real-time data and analytics. It has received numerous awards for its technology and customer support, including consistently high Net Promoter Scores. Worldwide, nearly 4,000 enterprise organizations and 1 million users depend on it.

The NetMotion data used in this report is from consenting third parties and customers running its software or from its Employee Frustration Index, a survey of 285 individuals across a wide range of age groups and device types. All users and respondents were from within North America.

netmotionsoftware.com

Netskope

The Netskope Security Cloud, used by millions of users in thousands of accounts globally, provides visibility and near real-time data and threat protection when accessing cloud services, websites and private apps from anywhere, on any device. Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering some of the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey.

Netskope provided aggregated, anonymized data from the Netskope Security Cloud platform for this report.

netskope.com

Symantec, a Division of Broadcom

Mobile threat intelligence provided by Symantec Endpoint Protection Mobile (SEPM) is used to predict, detect and protect against a broad range of existing and unknown threats. SEPM's predictive technology uses a layered approach that leverages massive crowdsourced threat intelligence, in addition to both device-based and server-based analysis, to proactively protect mobile devices from malware, network threats, and app and OS vulnerability exploits.

symantec.com

VMware

VMware software powers complex digital infrastructure around the world. Its cloud, networking and security, and digital workspace offerings provide a dynamic and efficient digital foundation to customers globally, aided by an extensive ecosystem of partners. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough innovations to its global impact.

VMware routinely carries out Customer Advocacy studies, data from which was used in this paper.

vmware.com

Wandera

Wandera is a cloud security company that protects modern enterprises beyond the traditional perimeter. When remote users access applications from their smartphones or laptops, anywhere in the world, its unified security cloud provides real-time threat protection, content filtering and zero-trust network access. Wandera regularly shares the latest findings from its threat intelligence, which applies machine learning across 425 M worldwide sensors. Founded in 2012 by a team of cloud security veterans, it is headquartered in San Francisco and London, and is recognized as a leader by leading analyst firms.

Wandera researchers teamed with Verizon to investigate mobile security trends that covered one full year of real-world usage in customer environments. The devices included both bring-your-own (BYO) and corporate-liable platforms that were protected by a Wandera mobile security solution.

wandera.com

Back to table of contents ›

Law enforcement

Federal Bureau of Investigation (FBI)

The mission of the FBI's Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information concerning suspected internet-facilitated criminal activity, and to develop effective alliances with industry partners. Over the last five years, the IC3 has received an average of almost 300,000 complaints per year. These address a wide array of internet scams and cybercrime affecting victims across the globe.

fbi.gov

United States Secret Service

The U.S. Secret Service has two core responsibilities: ensuring the safety of the U.S. President and Vice President, their families, and other designated individuals, events and locations; and safeguarding the nation's financial and payment systems. While the Secret Service is undeniably today better known for the first of these two responsibilities–physical protection–its history, traditions and expertise are all firmly rooted in its more than 150 years of conducting financial crime investigations.

As the global financial system has become increasingly integrated and digitized, the Secret Service has steadily turned its investigative focus to cyberspace, where the most significant financial crimes threatening the integrity of the U.S. economy are now committed. Consequently, over the course of the past 30+ years, the Secret Service has built a reputation for countering the most sophisticated and profitable cybercrimes, and for apprehending some of the world's most notorious transnational cybercriminals.

secretservice.gov

Back to table of contents ›

References

1 Based on survey commissioned for this report (see methodology section). Question asked of 75 respondents in the retail, hospitality and travel industries.

2 U.S. State Comprehensive Privacy Law Comparison, Mitchell Noordyke, IAPP, 2019, https://iapp.org/resources/article/state-comparison-table/

3 Mobile Malware: Public Awareness and Prevention, Europol, https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/mobile-malware

4 Based on observed actions in user base with sample size ranging from tens of thousands to tens of millions of users, Lookout, July 2019 to September 2019

5 Based on observed actions in user base with sample size ranging from tens of thousands to tens of millions of users, Lookout, July 2019 to September 2019

6 Based on observed actions in user base with sample size ranging from tens of thousands to tens of millions of users, data supplied by Lookout, July 2019 to September 2019

7 Christopher McMahon, U.S. Secret Service, 2019

8 High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, 2019, https://www.ic3.gov/media/2019/191002.aspx

9 Latest BEC Victims: Nikkei, City of Ocala, Bank Info Security, November 2019, https://www.bankinfosecurity.com/latest-bec-victims-nikkei-city-ocala-a-13351

10 Mobile Phishing Report, Wandera Threat Research, 2019, https://www.wandera.com/mobile-phishing-report/

11 Test carried out by a Lookout customer, 2019

12 Analysis of mobile phishing attack trends covering a diverse set of production devices in use across all represented regions, Wandera Threat Research, November 2018 and October 2019

13 Mobile Phishing Report, Wandera Threat Research, 2019, https://www.wandera.com/mobile-phishing-report/

14 Source images captured and supplied by Lookout, 2019

15 Investigation of mobile usage trends in company-managed devices where usage-based risks were of concern across whole customer base, Wandera, November 2018 to October 2019

16 VMware customer research, 2019

17 Travel Cybersecurity Study, based on online interviews with 2,201 U.S. adults weighted to approximate a target sample based on age, race/ethnicity and gender, IBM and Morning Consult, May 2019, https://www.ibm.com/downloads/cas/ZP95XZ6O

18 Analysis of mobile app permissions, including all apps installed on protected devices, regardless of download source, Wandera Threat Research, November 2018 to October 2019

19 Based on aggregated usage data, MobileIron, January 2019 to September 2019

20 Michael D’Ambrosio, Assistant Director for Investigations, U.S. Secret Service, 2019

21 Donna Gregory, Unit Chief, FBI Cyber Division, 2020

22 Assessment of the effect of cryptocurrency valuation on cryptojacking attack volume, including all cryptojacking incidents encountered by monitored mobile devices around the world, Wandera Threat Research, July 2018 to December

23 Customer case study: The impact of WhatsApp vulnerabilities on security posture over 6 months (May 2019 to October 2019), 2019 Wandera Threat Research

24 Based on aggregated usage data, MobileIron, January 2019 to September 2019

25 High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, FBI, 2019, https://www.ic3.gov/media/2019/191002.aspx

26 Travel Cybersecurity Study, based on online interviews with 2,201 U.S. adults weighted to approximate a target sample based on age, race/ethnicity and gender, IBM and Morning Consult, May 2019, https://www.ibm.com/downloads/cas/ZP95XZ6O

27 VMware customer research, 2019

28 Based on analysis of Symantec Endpoint Protection users, Symantec, January 2019 to December 2019

29 Analysis of common configuration vulnerabilities in production enterprise mobile devices, Wandera Threat Research, November 2019 to October 2019

30 X-Force Threat Intelligence Index, IBM, 2018, https://www.ibm.com/downloads/cas/MKJOL3DG

31 Data supplied by Wandera, November 2019

32 Data supplied by Wandera, November 2019

33 Based on aggregated usage data, MobileIron, January 2019 to September 2019

34 X-Force Threat Intelligence Index, IBM, 2018, https://www.ibm.com/downloads/cas/MKJOL3DG

35 Based on analysis of anonymized and aggregated data from customers and other third parties within North America, NetMotion, September 2018 to August 2019

36 Analysis of man-in-the-middle attacks and risky hotspots encountered by protected mobile devices, Wandera Threat Research, November 2018 to October 2019

37 Based on analysis of anonymized and aggregated data from customers and other third parties within North America, NetMotion, September 2018 to August 2019

38 Data gathered by Symantec from its base of users over a 90-day timeframe during 2019

39 Analysis of mobile data consumption by company-managed devices running the Wandera app, across domestic cellular, roaming cellular and Wi-Fi networks, Wandera Mobile Data Research, November 2018 to October 2019

40 Tech Tuesday—Holiday Travels, FBI, December 2019, https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdayholidaytravels

41 Michael D'Ambrosio, Assistant Director for Investigations, U.S. Secret Service, 2019

42 Data supplied by NetMotion, 2019

43 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019

44 Mobile Threat Catalogue, NIST, https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/mobile-threat-catalogue

45 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019

46 Based on analysis of anonymized and aggregated data from customers and other third parties within North America, NetMotion, September 2018 to August 2019

47 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

48 Mobile Threat Catalogue, NIST, https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/mobile-threat-catalogue

49 IoT connections outlook, Ericsson, 2019, https://www.ericsson.com/en/mobility-report/reports/november-2019/iot-connections-outlook

50 Cyber Actors Use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious Cyber Activities, FBI, August 2018, https://www.ic3.gov/media/2018/180802.aspx

51 Based on anonymized data from base of more than 10,000 enterprise customers, Asavie, January 2019 to September 2019