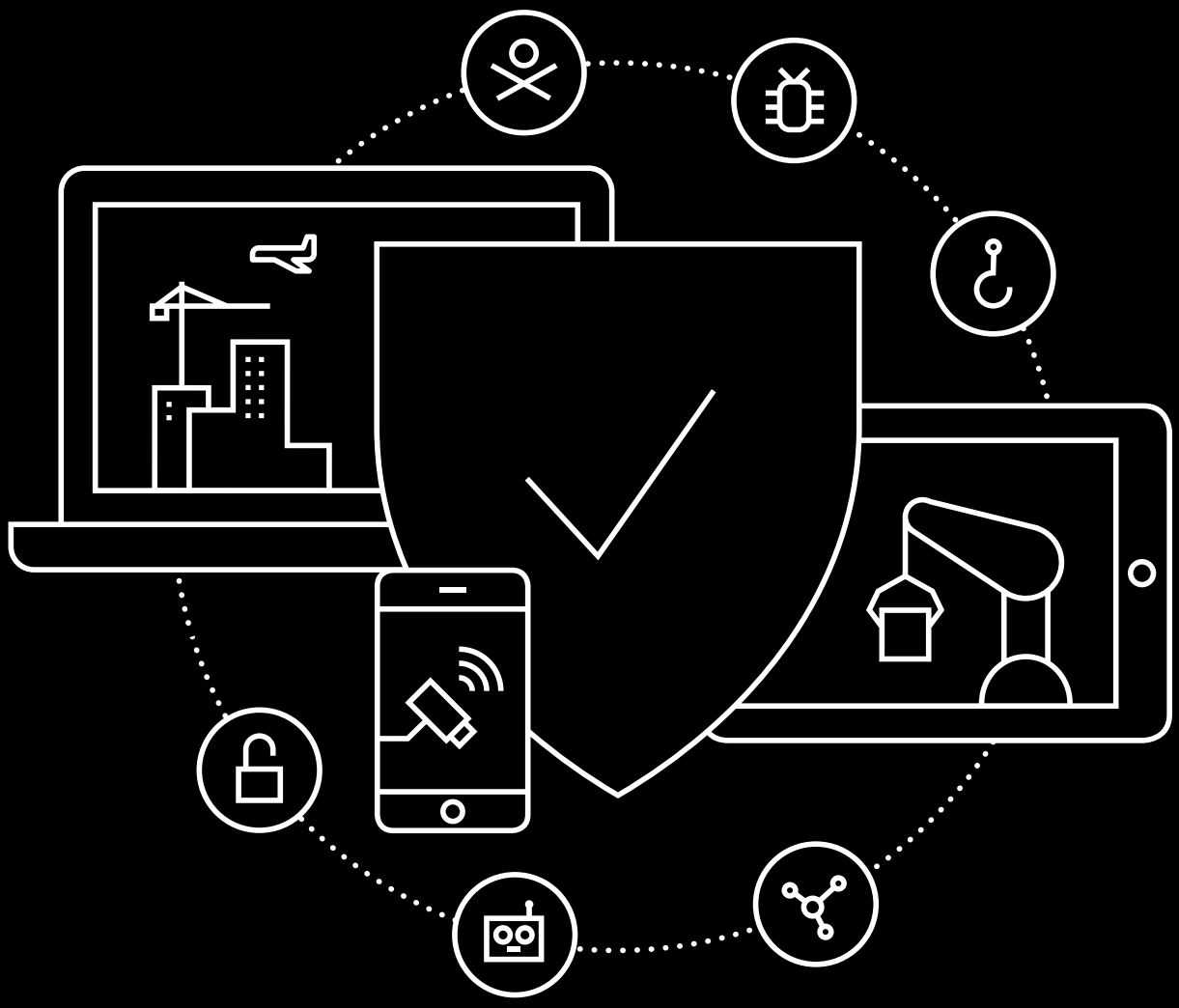
It's time to tackle mobile security.



verizon business ready

Foreword

It's been another headline-grabbing 12 months for cybersecurity. There were many large and damaging compromises affecting retailers, airlines and credit rating companies, to name just a few. Thousands of organizations weren't prepared and had sensitive data stolen, suffered downtime of key systems or were affected in some other way. Are you ready?

Something missing from the headlines was a compromise directly attributed to the vulnerability of a mobile device. Yet we found that the number of companies admitting they'd suffered a compromise in which a mobile device played a role went up – from 27% in the 2018 report to 33% this time around. So, where's the disconnect?

The answer lies in how little is normally made public about major incidents. We learn about the consequences – for example, how many thousands of social security numbers, or what secrets were exposed – but not the details of how it happened. Often, attacks will start with phishing, getting an unsuspecting user to click on a malicious link. But that part of the story rarely makes it into print, never mind whether it was actually a tap on a mobile screen rather than the click of a mouse. You could say that none of the biggest breaches have been publicly attributed to mobile vulnerabilities; but a mobile element hasn't been ruled out either.

Governments are starting to step in to make sure that organizations take cybersecurity across all endpoints more seriously. Since the publication of our Mobile Security Index 2018, we've seen the European Union's General Data Protection Regulation (GDPR) come into force and California legislate minimum standards for the security of connected devices. More legislation is likely to follow.

Our research shows that this is starting to focus attention – the threat of multi-million, even multi-billion, dollar penalties tends to have that effect. But cybersecurity, and mobile device security in particular, cannot wait for regulation.

And yet, companies are leaving mobile devices exposed to a degree they'd never tolerate elsewhere. Two thirds (67%) of organizations said they are less confident about the security of their mobile assets than other devices. That may have been tolerable when there was a huge gulf between what data mobile and fixed devices had access to – but that gap has shrunk, even closed completely.

Mobile devices now have access to much of the same valuable corporate data – customer lists, bank details, employee personal data, billing information and much more – as those using fixed connections. And many also hold the credentials that we use to access other resources, including the numerous cloud services that employees now depend on to do their jobs.

That explains why our survey found that so many companies suffering mobile-related compromises rated them as very serious. More than two fifths (41%) of those affected described the compromise as "major with lasting repercussions," and even more (43%) said that their efforts to remediate the attacks were "difficult and expensive."

The compromise of a mobile device can now be just as great a risk to your customer data, intellectual property and core systems. It's time to close the chasm between the levels of protection.

Thomas T. J. Fox

SVP & President Business Markets

Verizon

To help you assess your own environment and calibrate your mobile defenses, we've produced this updated Mobile Security Index. As last time, we surveyed nearly 700 professionals involved in buying, managing and securing mobile devices for their organization. To add additional insight, we worked with IBM, Lookout, MobileIron and Wandera, all leaders in mobile security and management. They provided additional data, including incident and usage data. We'd like to thank them for their valuable contributions in helping us present a fuller picture of the threats impacting mobile devices and what is being done to mitigate them.

Contents

Terminology

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 just accessing it without permission.
Compromise	A successful attack that results in a system’s defenses being rendered ineffective. This could result in data loss, downtime, other systems being affected or nothing at all. It could be malicious or accidental.
Data breach	An incident that results in the (potential) disclosure of data.
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 non-malicious 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.

Contents

Survey highlights

The security risks have gone up, and continue to grow.

83%

Five of six respondents said that their organization was at risk from mobile threats. 29% said that it was a significant risk.

The risks associated with mobile devices have grown

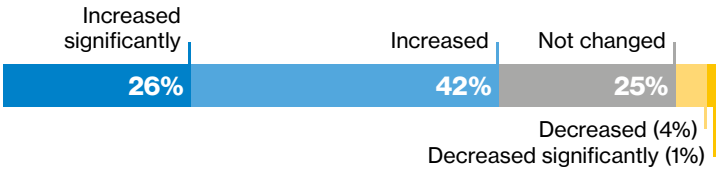


Figure 1. How do you think the security risks associated with mobile devices changed in the past year?

And they believe the risks are rising: 69% said that they'd grown in the past year. This reflects not just greater appreciation of the threats, but also the growing reliance on mobile devices and their increased access to other corporate resources.

Mobile threats are growing faster than others

Figure 2. Mobile device security threats are growing more quickly than others.

On average, 86% agreed that mobile threats are growing more quickly than others. Looking across industry groups, that number never dropped below 80%.

Across industries, 80%+ think mobile threats growing faster

Figure 3. Mobile device security threats are growing more quickly than others.

Jump to page 8 to read more about the threats.

But companies said their defenses aren't keeping pace.

67%

To make matters worse, two thirds of organizations said they are less confident about the security of their mobile assets than other devices. A fifth (21%) strongly agreed with that statement.

85%

And five of six said organizations need to take mobile device security more seriously.

Companies of all sizes agree on the need to do more

Figure 4. Do you agree with the statement "Organizations need to take mobile device security more seriously"?

Across the board, from the smallest companies we surveyed to the largest, there was widespread agreement on this. 90% of those in senior management roles also agreed.

Majority in each industry less confident about mobile security

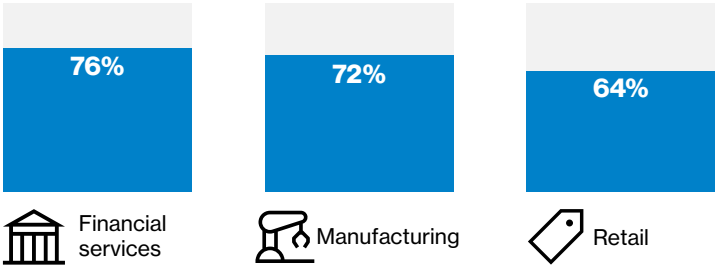


Figure 5. Do you agree with the statement "I'm less confident about the security of our mobile devices than other systems"?

Again, financial services companies were the most likely to concur.

See page 26 for the full industry breakdown.

And they were still cutting corners.

48%

Though they're aware of the threats, a growing number of organizations are putting speed and profit before mobile security. Almost half said they had sacrificed security to "get the job done," up from 32% last year.

Across industries, around half have knowingly cut corners

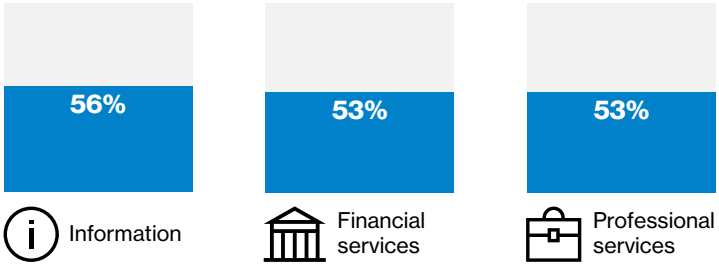


Figure 6. Has your organization ever sacrificed mobile device security to "get the job done" (e.g., meet a deadline or hit productivity targets)?

And that figure is fairly consistent across industries. The outlier is public sector, where just over a quarter (26%) said they'd put expediency before protecting data and systems.

See page 26 for the full industry breakdown.

Only 12% of companies had all four basic protections in place

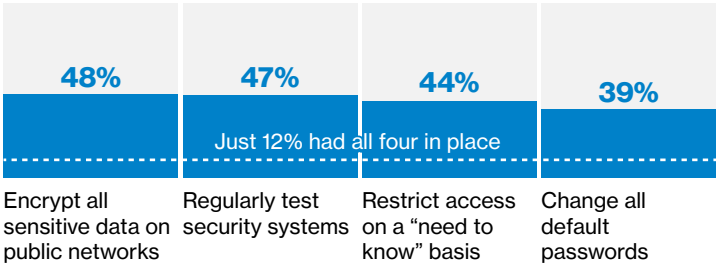


Figure 7. Which of the following match your organization's security policies?

Organizations are still failing to take the most basic security precautions. Less than one in seven (12%) organizations had all four of the most basic precautions in place – that's down two percentage points (2pp) from the 2018 report.

Skip to page 23 to read our recommendations for improving your mobile security.

The result? More organizations were hit, and hit harder.

33%

The percentage of organizations that admitted to having suffered a compromise involving a mobile device increased, and the impact of these attacks has been significant. A third said they'd experienced a compromise, up from 27% in the 2018 report.

46%

Nearly half of those that sacrificed security admitted to suffering a compromise. Less than a quarter (24%) of those that hadn't sacrificed security said the same.

62%

And these weren't trivial, nuisance incidents. More than three fifths of the companies affected described the compromise as "major." And over two fifths (41%) described the compromise as "major with lasting repercussions."

The impact of mobile attacks can be far-reaching. Of those admitting that they'd suffered a compromise involving a mobile device, most experienced more than one consequence:

The loss of data is only part of the problem

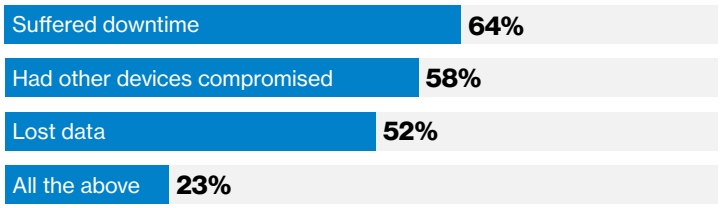


Figure 8. Which of the following consequences did your organization experience as a result of that security breach?

43%

Over two fifths said the actions required to remediate security incidents were "difficult and expensive."

Jump to page 8 to read more about the threats.

The perception gap

We found that companies are surprisingly confident in their mobile defenses. This isn't simply a lack of awareness of the dangers – they are concerned about the security of their mobile devices. But their confidence in their existing precautions isn't borne out by the number that fell afoul of a compromise.

Most agreed that mobile security is an issue.

The vast majority of organizations are aware that mobile devices pose a threat. Five of six (83%) said their business faces at least a moderate risk from mobile security threats. Almost a third (29%) said that the risk is significant.

> According to MobileIron, in the first half of 2018, 31% of active mobile devices recorded threats[1].

In fact, many rank mobile devices as their biggest cybersecurity concern. Over two fifths (41%) said that they are most concerned about mobile devices. This goes up to nearly half (49%) if you include Internet of Things (IoT) devices, many of which use radio-based connectivity.

Mobile devices topped organizations' list of concerns

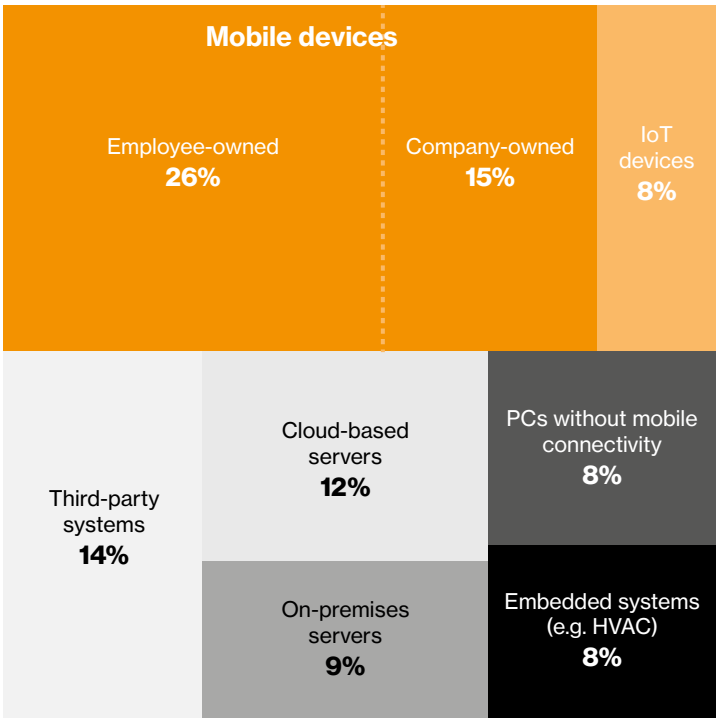


Figure 9. Please rank the following in terms of the security risk you think they present to your company.

Organizations said they trust their defenses.

Despite the perceived risk and the majority of respondents in each industry saying that they were less confident in their mobile defenses, most still thought that their mobile security measures were effective.

> Based on an analysis of privacy and security settings, 38% of mobile devices introduce unnecessary risk into the organization[2].

Companies said their existing mobile security is effective

Figure 10. How effective are your organization's current mobile security measures?

83% rated their existing mobile security measures as "effective," including a third (33%) that thought that they were "very effective."

No defenses are invulnerable. It's critical that organizations are able to spot incidents quickly and shut them down before attackers have time to do material damage.

Organizations were confident they'd spot a problem quickly

Figure 11. Are you confident that if a mobile device was compromised it would be spotted quickly?

Almost four in five (79%) said that they are confident that they'd spot a compromised mobile device quickly.

Companies were confident they'd spot misuse quickly

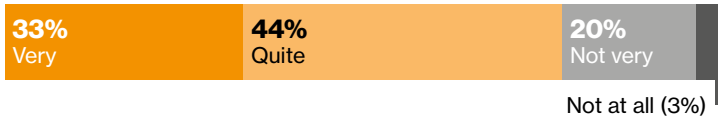


Figure 12. If one of your employees misused a company mobile device (e.g., used it to access inappropriate content), how confident are you that it would be spotted quickly?

And a similar percentage (77%) were confident that they would spot misuse by employees promptly.

This sentiment is not matched by events or actions.

A third (33%) of organizations admitted that they have experienced a compromise that involved a mobile device – up from 27% in the 2018 report.

Many incidents were serious in nature

Figure 13. How serious was the impact of the mobile-device-related security incident(s)?

This can't be accounted for solely by lost devices and relatively harmless things like adware infections. Three fifths (62%) of those that experienced a compromise described the event as "major," and 41% said that it had lasting repercussions.

Many compromises were difficult and expensive to correct

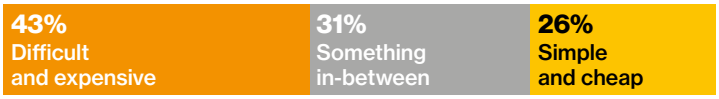


Figure 14. How would you describe the actions required to mitigate the incident?

Further, over two fifths (43%) said that measures to mitigate and remediate the incident were "difficult and expensive."

Most companies found out from a third party

Figure 15. In which of the following ways were you made aware of the breach?

And refuting the belief that problems would be spotted quickly, the majority of organizations were made aware of a compromise by a third party – such as a customer, partner or law enforcement.

Many organizations didn't have early detection systems

Figure 16. Which of the following security measures do you use to detect and mitigate mobile device security threats?

That's not really surprising, as we found that many organizations didn't have the systems in place that would enable them to reliably detect and mitigate incidents quickly.

The adoption of many key mobile security solutions is low

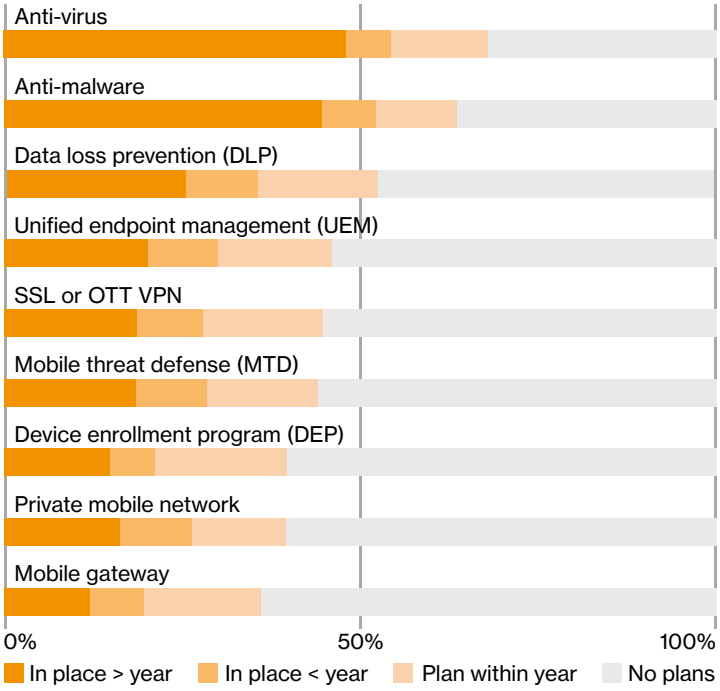


Figure 17. Which of the following security measures do you use to detect and mitigate mobile device security threats? Have you had this security measure in place for a year or more? Do you have plans to implement the following within the next 12 months?

Just as we found in the 2018 report, the adoption of key protections, like anti-virus and UEM, is low.

Far more respondents said that they plan to implement each of the mobile security protections mentioned above in the next 12 months than had done so in the previous 12. We could interpret this as more companies having realized the need to improve their defenses and starting to take action. But a comparison with last year's stats suggests that this is more likely to be over confidence. While they may hope, and even plan, to introduce additional protections, many will fail to do so.

What's in a name?
MTD, MTM, MTP, MDM, it's a bit of an alphabet soup. For the purposes of this report we've used three groupings:

Device enrollment programs (DEP) – focused on device deployment.

Unified endpoint management (UEM) – including mobile device management (MDM) and enterprise mobility management (EMM).

Mobile threat defense (MTD) – focused on detecting and mitigating threats. Includes mobile threat management (MTM) and mobile threat protection (MTP).

Actors, motives and threats.

The who and why are familiar—certainly to any regular reader of Verizon's Data Breach Investigations Report (DBIR)[3]. Employees and organized criminal groups top the list of perpetrators companies are most concerned about. When it comes to the tactics used, the usual suspects—phishing, ransomware etc.—are there. In fact, mobile devices can be more susceptible to some of these threats. But there are also many mobile-device-specific dangers, like rogue Wi-Fi.

Actors and their motives

Actors: Who are the "bad actors"?

While organizations are concerned about professional criminals, hacktivists and state-sponsored actors, they're even more worried about threats from within.

Employees topped the list of actors that worry companies

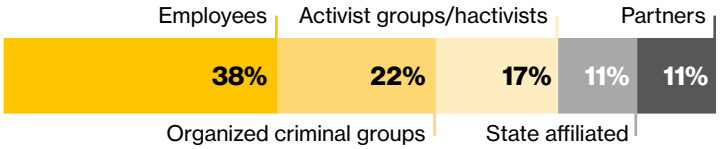


Figure 18. Which of these are you most concerned about?

At 38%, employees topped the list of actors that respondents were most concerned about. Members of staff frequently expose their organizations to risk, both knowingly and unknowingly. Included in this number is the issue of negligence – employees making careless errors, losing their devices, using public Wi-Fi or circumventing security rules.

> Attackers are adapting to the mobile-first world and expanding their arsenals. 51% of sophisticated actors identified in the last 12 months were found to be targeting mobile devices as well as desktops[4].

Organized criminal groups weren't far behind. These groups are constantly adapting. As one type of IT system becomes less vulnerable, they will move on to another. And they are constantly finding new ways to make money from their efforts. While "smash and grab" attacks are still common, there are much more sophisticated attacks, too.

> In November 2018, a large international hotel chain announced that it had suffered a data breach affecting up to 500 million guests. Perhaps most alarmingly, the company admitted that the attackers had gone undetected since 2014[5]. The DBIR has reported on the time between compromise and detection, and it's common for this to be measured in weeks or even months. Advanced persistent threats like this are growing increasingly sophisticated. Attackers will adapt their methods and repeatedly target the same company; and once they are in, they will seek to move from system to system to do more damage and/or increase their financial gain.

Motives: What's driving them?

It's hardly surprising that personal gain tops the list of motives companies are concerned about. This finding mirrors what the DBIR has found year after year for more than a decade.

Nor is it a shock to see "unintentional" come in second, considering that employees are who organizations were most concerned about. Likewise, with "convenience," we've already talked about companies cutting corners to get the job done. Well, they worry about their employees doing it too.

Personal gain was the most frequently cited motive

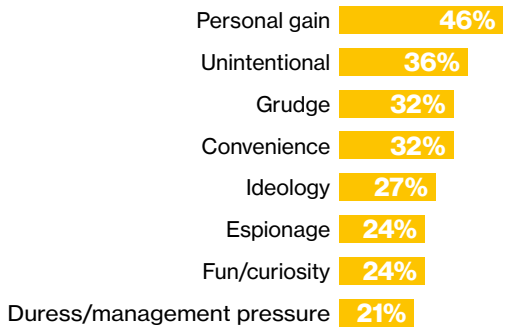


Figure 19. Which of the following motives for attacks are you concerned about?

When it comes to malicious actions – whether they're perpetrated by employees, ex-employees or complete strangers – organizations are more worried about those committed as part of a grudge (32%) than those driven by ideological reasons (27%).

Threats: What tactics are they using?

We've broken threats and vulnerabilities into four layers: user-behavior-based, app-based, device-based and network-based.

Malware was foremost among respondents' concerns

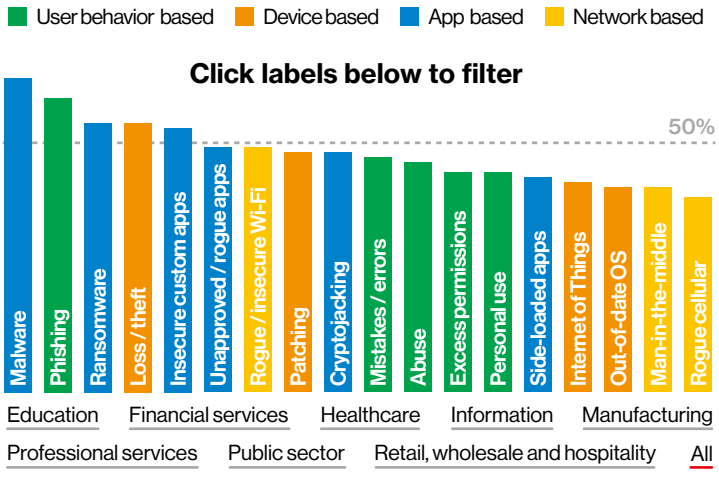


Figure 20. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

We cover each of these in more detail on the coming pages.

User behavior threats

Many threats come down to things that users do. This might be breaking policy, using a device for personal use, clicking on a malicious link, or installing an app and giving it permissions it doesn't need.

Respondents were aware of and concerned about

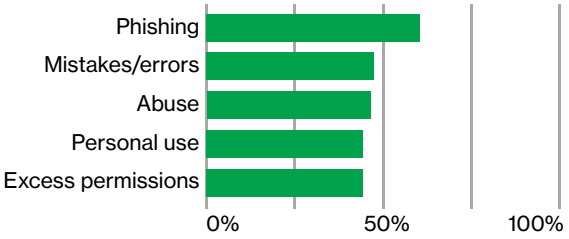


Figure 21. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

Abuse/personal use

Less than a fifth (19%) had a fully comprehensive AUP

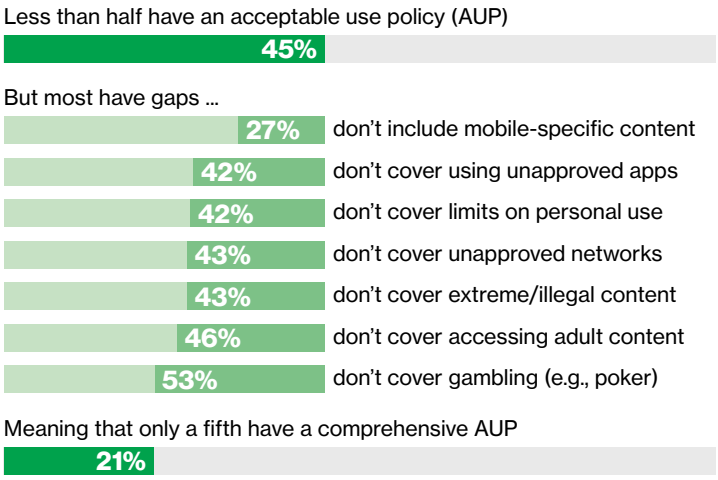


Figure 22. Which of the following do you have in place? Which of these has mobile-device-specific content? Which of the following are covered in your acceptable use policy (AUP)?

What constitutes improper use of a company mobile device? There's no agreement on what kind of employee behavior is appropriate and what isn't. There are also many gray areas – for example, when a mobile device is owned by the employee, but is used to access corporate resources or perform work tasks on a regular basis.

To clarify this uncertainty, we break the problem down into three categories:

- Misuse of corporate resources
- Accessing inappropriate content
- Exposing company data and assets to increased risk

Misuse of corporate resources
Defining what constitutes misuse of corporate resources can be tricky. For example, some companies will frown on the use of social media, but many others encourage employees – especially salespeople – to use it to do their job more effectively. How can companies differentiate between watching a cute cat video and an interview with the CEO of a customer?

Two thirds (66%) of respondents said that they are concerned, a quarter (25%) very concerned, about the volume of mobile data being used by their organization.

After deploying a mobile policy management solution to its 80,000 employees, one company saw the consumption of mobile data for personal use drop by a third. At the same time, the percentage of time spent on business apps went up significantly. These changes happened immediately after roll-out, before the company had actually deployed any policies. Just knowing that monitoring would be happening was enough to change behavior. Now that it has policies in force, the company can identify and correct non-compliance automatically[6].

Accessing inappropriate content
Regardless of whether material is inherently dangerous, most organizations wouldn't be happy about employees accessing inappropriate – adult, extreme or illegal – content on one of their corporate devices. Even when nobody else is going to see it over their shoulder.

Exposing company data and assets to increased risk
Finally, there's the threat of malicious content. Not safe for work apps and sites may or may not be more likely to harbor malware and other threats; but by accessing any kind of non-work content, employees are still increasing the danger to the organization's data and systems.

Over three quarters (77%) of organizations said they are confident that they can quickly spot an employee misusing a corporate device. But that doesn't align with what Wandera is seeing in real life. Take our self-assessment on the next page to see how likely it is that misuse is happening in your organization.

Self-assessment: Are your employees accessing inappropriate or dangerous content?

Look up your number of employees in the chart to see how likely it is that inappropriate content is being accessed on your organization's mobile devices.

It's interesting that typically the percentage of users accessing inappropriate content is lower in larger organizations; but because they have more employees, it's more likely that at least one is breaking the rules.

Type of content	Number of employees 100–249	250–499	500–999	1,000–4,999	5,000+	
Adult	14%	17%	14%	12%	10%	Users
	98%	99%	100%	95%	100%	Organizations
Extreme/illegal	1.0%	0.9%	0.9%	0.8%	0.5%	Users
	13%	55%	78%	85%	87%	Organizations
Gambling	16%	17%	17%	16%	10%	Users
	96%	97%	100%	95%	100%	Organizations
Gaming	44%	45%	47%	48%	33%	Users
	99%	98%	100%	100%	100%	Organizations

Data provided by Wandera[7]

Excess permissions

We all know that few people read the lengthy terms and conditions when upgrading the OS on a device or installing a new app. The page that lists what permissions an app wants is typically much shorter, but do users still just click "Ok" anyway?

According to Lookout, 39% of mobile apps contain code that can access the device's microphone[8].

It is hard to believe that one in four apps need access to the camera (25%) – and that's at the bottom of our list. Some will have valid reasons: from social networking apps, through photo editing apps, to process automation apps – like those that capture pictures of receipts to automate expenses claims. But it's likely that many don't need all the access they have.

In many cases there will be a legitimate reason for requesting superfluous permissions – such as supporting planned new features. But even if the intent isn't malicious, these unnecessary permissions could be exploited. Access to the camera could be (mis)used for surveillance or to capture passwords as users enter them; the microphone could be used to eavesdrop on conversations. Even access to the calendar or contacts list could be abused. For example, stolen information can be used to send more-targeted phishing emails, leveraging the fact that people are more likely to open a message that appears to be from someone they know.

Lots of apps have access that could be abused

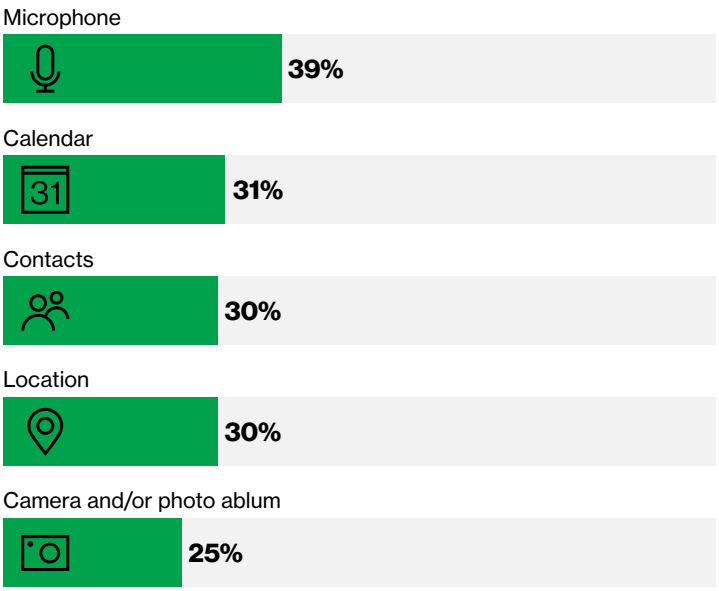


Figure 23. Share of iOS apps with access to features which could be misused[9].

Behind the scenes, many apps are also gaining access to low-level functions. Wandera found that one in eight (12%) Android apps request permission to "modify system settings" and 90% request "full network access" – this isn't necessary for normal connectivity, but enables them to create network sockets and use custom network protocols[10].

Phishing can spread quickly

Figure 24. Spread of variant of the L33bo phishing kit. Data provided by Lookout[11].

Phishing/business email compromise

Attackers often play a numbers game. They use automated tools and botnets to test the defenses of many thousands of devices. But some attackers take a more targeted approach. "Spear phishing" and business email compromise, also called CEO fraud, require more effort, but can be extremely effective.

Enterprise users are three times more likely to fall for a phishing link when on a small screen (Android or iOS device) than when using a desktop OS, like Windows or macOS[12].

Users are more vulnerable to phishing on a mobile device. Many of the protective measures people typically take are not as easy: Who looks for the padlock, or hovers over the link to see the underlying URL? And mobile devices are much less likely to have endpoint protection installed.

Over two fifths (42%) of respondents who said that they'd experienced a mobile-related compromise said it involved phishing.

Where phishing attacks happen on mobile devices

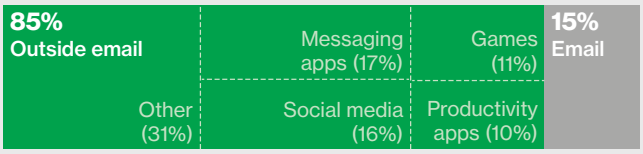


Figure 25. Locations of phishing attacks on mobile devices.

85% of phishing attacks seen on mobile devices take place outside of email. While many organizations have filtering in place to block email-based attacks, far fewer have similar protection in place for these other routes[13].

Phishing kits make it easier for even those without advanced technical skills to create effective campaigns and become a cybercriminal. The map above shows the spread of attacks using just one kit, L33bo, over 24 hours in 2018. Even months after it became known, dozens of companies and individuals were still being caught in its net each week[14].

The FBI's Internet Crime Complaint Center (IC3) reported that victims of internet crime lost over $1.4B in 2017. 48% of that was due to business email compromise[15].

App threats

It's not just obviously questionable apps and websites that organizations need to worry about. App threats come in many forms. Even mainstream enterprise apps downloaded from the manufacturer's app store can be compromised or suffer from poor coding practices.

Respondents were aware of and concerned about

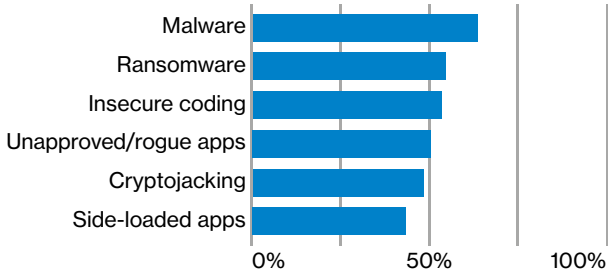


Figure 26. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

Malware

Malware remains at the top of the list of threats that organizations are most concerned about, followed by ransomware. As well as "traditional" malware, our contributors have noticed an increase in attacks targeting two-factor authentication apps.

According to Lookout, 4.1% of its users have encountered malicious apps[16]. Similarly, MobileIron found that 3.5% of Android devices harboured known malware. Of these malicious apps, over 80% had access to internal networks and were scanning nearby ports. This suggests that the malware was part of a larger attack[17].

Companies are well aware of the dangers of malware, but again aren't taking the obvious precautions – like deploying a mobile threat defense solution.

In a four-week trial, 0.03% of all mobile devices encountered a malicious app[18]. This might seem trivial, but it's far from it. This means that an organization with just 250 devices has a 7% chance of at least one device becoming infected in a four-week period, and a 62% chance over the course of a year. The self-assessment, right, shows the likelihood of at least one device being infected by company size.

Websites and webapps – even those connected to reputable companies – can also expose users to malicious code. There have been several high-profile examples of this recently, including well-publicized incidents involving two international airlines – each their country's trusted flag carrier.

While there's no evidence that these attacks targeted mobile devices, mobile users will inevitably have been caught up in them. This is another example of how mobile devices can be susceptible to many of the threats aimed at other devices, as well as attacks that exploit mobile-specific vulnerabilities.

There are many features of mobile devices that potentially make users more vulnerable to these attacks:

- There's no mouse-over or preview functionality to enable the user to evaluate the destination before clicking
- Smaller screens make it harder to evaluate the legitimacy of a website
- As the user scrolls down, the address bar is often hidden to make more room for page content

Some attackers have exploited Punycode (used to handle non-Latin characters in domains) to trick users. For example, most browsers will display xn--rolx-nu5a.com as rolex.com[19].

Self-assessment: Do you have infected devices right now?

Look up how many mobile devices your organization has in the chart below. The upper and lower bounds show how likely it is that at least one of them is infected.

Number of devices	Likelihood of having at least one device infected with a malicious app
100–249	3% – 7%
250–499	7% – 14%
500–999	14% – 26%
1,000–2,499	26% – 53%
2,500–4,999	53% – 78%
5,000–9,999	78% – 95%
10,000+	95% – 100%

Data from Wandera[20]

Ransomware

We suspect that ransomware appears so high on the list due to the widespread media coverage of high-profile, global attacks like WannaCry and CryptoLocker. Though as these were pretty "successful," it's not a bad thing that companies are taking note.

Over 40% of all successful malware-based attacks involved ransomware[21].

Greater awareness has encouraged people to be more vigilant and better prepared, but attackers have evolved too. Numerous variations have been identified, including faux ransomware that doesn't really encrypt your files, deleteware (yep, erases your data), and doxware (instead of deleting files, publishes them online).

There are mobile-specific forms of ransomware. Typically, these target the Android platform as, traditionally, it has exercised less control over the installation of third-party apps – although this is changing. At least one form of ransomware targeting iOS has been identified[22].

The evolution of ransomware

Android crypto-ransomware dates back to Simplocker, first discovered in June 2014.

In its early days, Simplocker was easy to mitigate. It used a single hardcoded encryption key. Once the key was identified, it was possible to unlock any infected devices.

More recent versions create a unique encryption key for each device they infect. This makes it considerably more difficult to mitigate.

Ransomware authors have also adopted new ways of spreading their wares. Spam emails and infected websites were once the favorite ways to get malware onto devices, but attackers are now using a wide variety of techniques, including corrupted versions of apps on third-party app stores and even text messages.

These examples show how ransomware can be redesigned and new deployment methods used to increase effectiveness and extend its life.

Unapproved/rogue apps

Over a random seven-day period, IBM detected more than 7,000 new Android apps and 11,000 new iOS apps[23]. With so many new apps appearing, it would be next to impossible to ensure that none of them did anything dangerous – even if there wasn't malicious intent. Yet, companies are surprisingly trusting.

Most companies let users install apps they haven't vetted

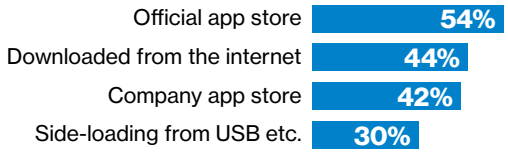


Figure 27. Which methods of installing apps does your organization permit?

Only two fifths (40%) of organizations said they limit users to installing apps from a recognized app store (like the Google Play Store or an internal one). And just 3% totally blocked users from installing apps.

Insecure coding of custom apps

The majority (70%) of respondents said that their organization has a custom app – specifically an internal one, not including those built for customers. Over half (53%) of those are concerned about the dangers of insecure coding.

OWASP (Open Web Application Security Project) has identified the top 10 ways in which cybercriminals compromise mobile apps[24]:

1. Exploiting the misuse of a platform feature or failure to use platform security controls properly
2. Accessing information that was held in insecure storage or leaked unintentionally
3. Compromising authentication due to weaknesses in handshaking, SSL versions, cleartext communication etc.
4. Gaining access due to failure to identify the user at login and during use
5. Exfiltrating sensitive information due to insufficient encryption
6. Exploiting insecurities in authorization to gain access
7. Taking advantage of input handling issues, including buffer overflows, to affect the proper running of code
8. Tampering with code through binary patching, local resource modification, or dynamic memory modification
9. Using binary inspection tools to snoop on the inner workings of the app – this can be used to identify vulnerabilities and to reveal information about other assets and authentication/cryptography
10. Exploiting extraneous functionality, such as hidden backdoors, that were not meant to reach the production environment

Cryptojacking

Cryptojacking can reduce device operating time by up to 65%

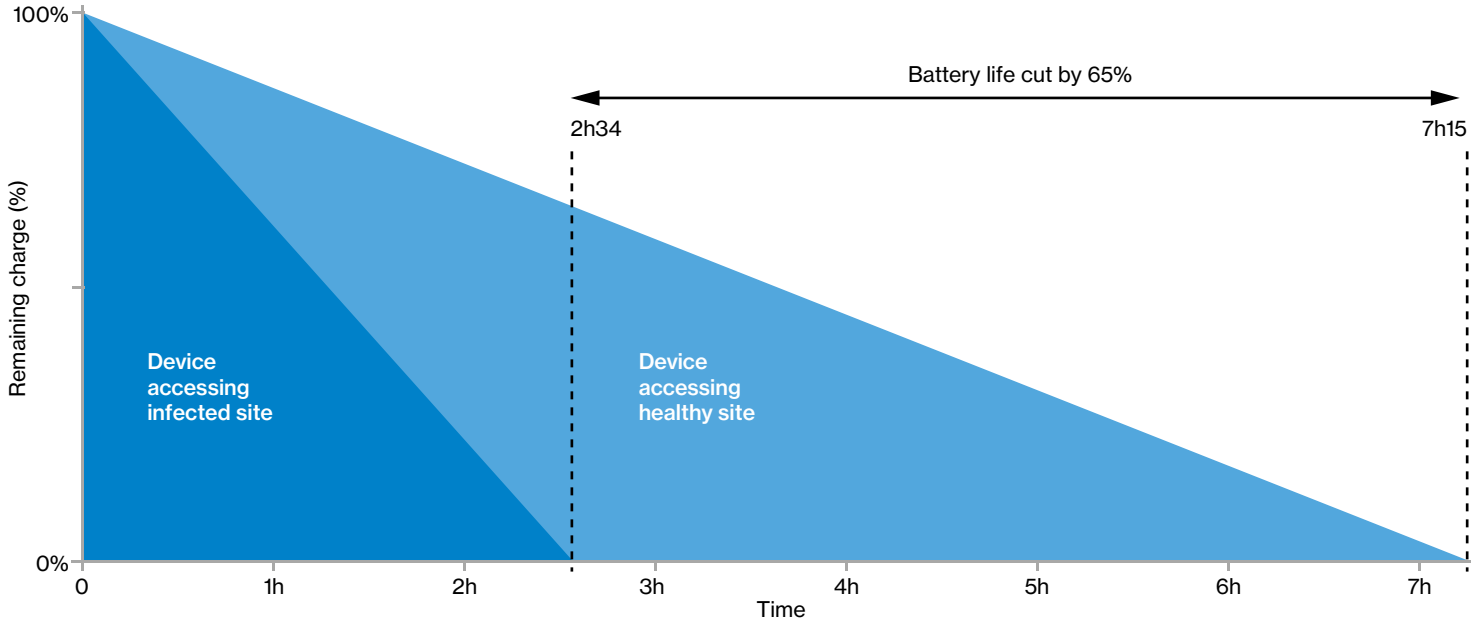


Figure 28. Cryptojacking test exercise conducted by Wandera[25].

A quarter of companies have encountered cryptojacking

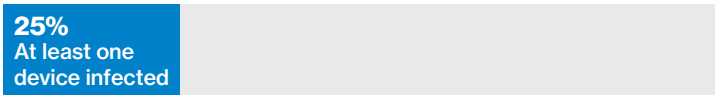


Figure 29. Prevalence of cryptojacking[26].

In 25% of companies at least one mobile device has encountered cryptojacking. Infections are typically invisible and don't steal data or hijack credentials. But they aren't harmless.

> Cryptojacking – the unauthorized use of a third party's device to mine cryptocurrency – started out as a legitimate source of revenue. Coinhive used JavaScript on websites as an alternate means of paying for access – processing time instead of cash. Sadly, cybercriminals were quick to see the potential of hiding similar code on sites and within apps.

In a test exercise (see Figure 28), Wandera measured the charge of devices accessing normal "healthy" sites and ones infected with a cryptojacking script over time. It found that operating time was cut by up to 65%. But that could be just the tip of the iceberg.

The impact of even an "innocuous" infection can be severe. It could trigger detection systems and shut down a line or ground a plane. But the consequences of letting an infection through, even if it looks harmless, could be much worse.

Self-assessment: Are your mobile devices more exposed?

Are you leaving your mobile users more exposed? Circle "yes" or "no" for each precaution your company has deployed, on desktops and on mobile devices.

Defense	Desktops?	Mobiles?
Anti-malware/anti-virus	Yes / no	Yes / no
Data loss prevention	Yes / no	Yes / no
Endpoint protection	Yes / no	Yes / no
Firewall (device)	Yes / no	Yes / no
Firewall (perimeter)	Yes / no	Yes / no
OS integrity monitoring	Yes / no	Yes / no
Vulnerability scanning	Yes / no	Yes / no
Web filtering	Yes / no	Yes / no

Do your answers show that you are doing a lot more to protect your desktop devices than your mobile assets? In our experience, many companies are doing more to protect fixed devices than mobile ones. But as we rely on mobile devices more, and they are used to access more corporate resources – including ERP and CRM systems – shouldn't they be given equivalent protection?

Device threats

Each year millions of devices go missing. Most probably don't pose a threat, but it only takes one to expose confidential data or offer unauthorized access to other corporate resources. And then there's the challenge of keeping numerous different types of device – including phones, embedded systems, and many others – patched.

Respondents were aware of and concerned about

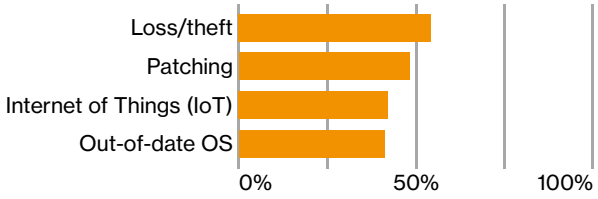


Figure 30. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

Device loss and theft

There doesn't need to be any malicious intent for companies to suffer a loss of data and even downtime. People lose stuff. They leave smartphones, tablets and even laptops on planes, trains, taxicabs and ride shares.

According to security device manufacturer Kensington, 70 million smartphones are lost each year, and only 7% are recovered. And specifically in the business world, 4.3% of company-issued smartphones are lost or stolen every year[27].

The prevalence of loss and theft is high, but it ranks quite low on the list of what companies are concerned about. This is probably because it's relatively easy to put right. It's seen as an unavoidable fact of life.

1–2% of all mobile phones/tablets don't have a lock screen configured. This increases to 5% of Android devices within companies with 500–999 employees[28]. This really is one of the most basic precautions companies can put in place, but is quite an effective protection against a lost/stolen device leading to a compromise. This suggests weak policies and/or ability to enforce those policies.

Supporting our hypothesis that companies' actions don't correspond with the real threat level, there is no correlation between being concerned about loss and theft and implementing whole disk encryption (WDE). Less than a third (31%) of both groups, concerned and unconcerned, have implemented this measure – included in Windows (BitLocker) and macOS (FileVault) – which can render the data on stolen disks worthless.

Less than half (48%) of companies using MDM enforce a lock screen on all devices[29].

Internet of Things (IoT) devices

Over three quarters of respondents said that they think IoT devices are the greatest cybersecurity threat facing organizations. A lot of the issues with protecting IoT devices stem from difficulties accessing and managing them.

Most companies agreed that IoT is the greatest security risk

Figure 31. Do you agree with the statement "IoT devices are the greatest security risk facing organizations"?

Many IoT devices don't have the same fundamental security features that are typical of smartphones. A lot simply don't have the storage or processing capacity to run traditional methods of protection.

And because they often operate in remote locations, they can be susceptible to physical tampering and be harder to patch.

It's not just the IoT devices and the data that they capture that are at risk. There have been many instances reported where IoT devices have been used as an entry point to critical systems and other sensitive or valuable data.

Downtime was a very common result of a compromise

Figure 32. Which of the following consequences did your organization experience as a result of that security breach?

Attackers could also use IoT devices to disrupt operations and cause downtime. This was a consequence of nearly two thirds (64%) of compromises reported by our respondents.

As well as the more familiar, and widely reported, attacks where data is stolen or held ransom, attackers can also use IoT devices to modify or corrupt data.

Out-of-date operating system

It's not just about major versions – like iOS 12 and Android Pie. With new threats and vulnerabilities emerging all the time, even being a few minor versions behind could pose a significant risk.

Average Android device is running an OS over two years old

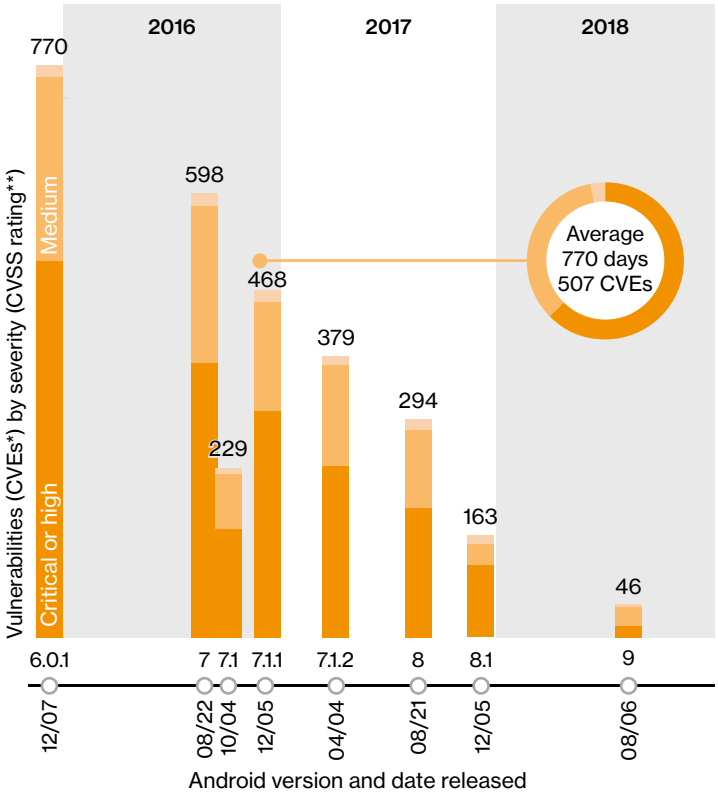


Figure 33. Age of device OS and corresponding number of CVEs[30].

Data from Wandera showed that 57% of Android devices were running an OS at least two full versions behind the current one. Mapping the known vulnerabilities of each version (based on CVEs* issued) and taking a weighted average, gave a mean of 507 known vulnerabilities per device. Nearly two thirds (63%) of these rated "critical" or "high" on the CVSS** scale.

Similar analysis of iOS devices – around two thirds (65%) of employee-owned devices are iPhones[31] – found that 67% were running a version less than six months old, and the average device had 17 known vulnerabilities, three of which were severe.

In 2018, 693 Android and iOS entries were added to the CVE database*. Over two fifths (43%) of these had a CVSS** score of 7 or greater, indicating they were severe and exploitable[32].

Patching

Except in very special circumstances, each device has only one OS. Most have tens or even hundreds of apps, making keeping them up to date a much tougher challenge.

Almost 5% of managed devices have over 100 apps installed[33].

It is critical to have an effective patching regime in place that not only monitors both the operating system and applications on a device but prioritizes and helps guide corrective actions when necessary.

Just one in two hundred (0.5%) Android devices are rooted and only one in a thousand (0.1%) iOS devices have been jailbroken[34]. While a relatively rare problem, these devices pose a serious threat. It's critical that companies detect these devices quickly, as they can be exploited to compromise other devices and core systems.

This patching regime should also address the issue of orphaned apps – those the developer has stopped maintaining but are still sitting on devices. These should be identified and the need for them and associated risk assessed.

Self-assessment: How effective is your patching program?

- Do you assess vendors' track records on patching when procuring software and devices?
- Do you use a discovery service to identify all appropriate patches and the severity of the issues they address?
- Do you have a scoring system for assessing and prioritizing patches?
- Do you measure your patch management?
- Do you measure it on the severity of issues patched, not just the number of patches that were deployed?
- Do you check that patches have been deployed correctly?
- Do you educate your staff on the importance of patching?

* Common vulnerabilities and exposures system maintained by The National Cybersecurity FFRDC, funded by Homeland Security.
** Common vulnerability scoring system, see https://nvd.nist.gov/vuln-metrics/cvss

Network threats

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

Respondents were aware of and concerned about

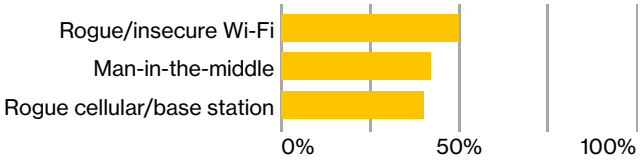


Figure 34. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

Insecure networks

Employees connect to an average of 12 Wi-Fi hotspots per day[35]. Unfortunately, not all access points can be trusted:

- Each month approximately 4% of devices encounter a risky hotspot (one known to be affected by man-in-the-middle, protocol attacks like SSL Strip, etc.)[36]
- Nearly 2% of mobile devices have connected to a rogue access point (one set up to imitate a legitimate network)[37]

Employees are taking risks, even when told not to

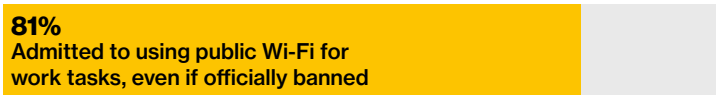


Figure 35. Do you use public Wi-Fi for work purposes?

Four fifths of respondents (81%) admitted to using public Wi-Fi for work, even when many know it's prohibited. When you look at just those respondents responsible for managing the security of devices, that figure is even higher (82%).

70% of Wi-Fi sessions were over an unencrypted connection[38].

This suggests that even the most savvy users let convenience take precedence over what they know is right, and they are prepared to risk the consequences. This supports our observation that actions don't match concerns.

Interception attacks

One of the most serious types of threat involves the interception of all network traffic. This can be achieved by creating a rogue access point or using a man-in-the-middle (MitM) attack. These techniques enable attackers to capture any data transmitted, including credentials, emails and data submitted to web forms.

Self-assessment: Would your users use these access points?

Many attacks take advantage of familiar public Wi-Fi names (SSIDs). Users may already have these stored in their device, which could try to connect automatically.

How many of these would you connect to without checking their legitimacy?

Southeastern_WiFi	The C1oud
Hilton Honors	Starbucks WiFi
hhonors	Airport_Free_WiFi_
McDonalds Free WiFi	Signature
Marriott_GUEST	Fairmont
PretCustomer	@Hyatt_WiFi
American Airlines lounge Wi-Fi	Courtyard_GUEST
starbuckz free wifi	Wifi_Guest

These SSIDs were among the most often identified by Wandera as exhibiting suspicious behavior, suggesting that they were actually being used by a rogue hotspot[39].

Note that some of these are misspelt – starbuckz? – giving the game away. Yet, users still connect to them.

And yet, just half of all companies had a solution in place to encrypt all traffic to protect users from this kind of attack:

- 28% were using an over-the-top (OTT) or SSL VPN
- 27% were using a mobile private network
- 21% were using a mobile web gateway

In the first half of 2018, more than one in seven (15%) protected devices detected an MitM attack[40].

What's being done.

Governments are taking IT security and privacy increasingly seriously. And we found that regulation is driving action. The industry is also working on hardening mobile standards and improving resilience. But many companies are still failing to take adequate precautions.

What governments are doing.

2018: The year of regulation.

The big regulation news of 2018 was clearly GDPR. It is by far the most ambitious and wide-ranging data protection law yet enacted. And while it's a European Union (EU) regulation, legislated by the 28 member nations, it has a global impact – any organization doing business in the EU, whether based there or not, is covered.

GDPR forced organizations to reassess mobile security

Figure 36. Do you agree with the statement "We have reassessed the risk associated with mobile devices in light of GDPR"?

In fact, we found that over three quarters (78%) of the US-based organizations that we surveyed said they had changed IT security policies in light of it. The well-publicized scale of potential penalties was almost certainly a driving factor.

But GDPR wasn't the only new kid on the block.

It received far less coverage, but the Directive on Security of Network and Information Systems (NIS) covers similar ground to GDPR and has the same maximum penalties. Unlike GDPR, it's left to individual countries to set their own thresholds; the UK has set its at £17M ($22M).

And in October 2018, California introduced new legislation[41] covering new connected devices, like smart home and other gadgets. Starting from 2022, companies manufacturing or selling devices in the state must include "reasonable" security measures. Among other things, it bans generic default passwords.

An example of attackers finding creative ways to monetize their efforts hit a UK national retailer[42]. Reports suggest that attackers tried many thousands of sets of credentials stolen from other sites on the retailer's website – a technique called "credential stuffing." As many people reuse usernames and passwords, many of these worked. But instead of creating fraudulent purchases, the attackers contacted the company and claimed to have hacked its system, using the accounts it had managed to access as "evidence." They then attempted to extort the retailer by threatening to expose the "breach," leaving the retailer liable to a consumer boycott and a GDPR fine, which could have been in the millions.

Regulation is not a panacea.

Some companies are still doing the bare minimum to comply with legislation and treating each compliance program as a standalone. This is inefficient and can damage effectiveness.

One of the recent airline breaches provides a good example. According to reports[43], payment card data was encrypted, but other sensitive personally identifiable information (PII) – like passport numbers – wasn't. It's fair to assume that this was because Payment Card Industry Data Security Standard (PCI DSS) stipulates that card data must be encrypted.

The threat of increased penalties has driven increased spend

Figure 37. Do you agree with the statement "The threat of increased regulatory penalties has been a major driver of increased security spending over the past year"?

Legislation can be good for us as individuals, if it discourages companies from failing to implement minimum standards. And regulations, like PCI DSS, can provide companies with a useful framework for building effective security programs. But neither should be seen as comprehensive, merely a baseline.

Read Verizon's Payment Security Report to find out more about PCI DSS and how to build a sustainable security compliance program, whether it's for PCI DSS, GDPR, the Health Insurance Portability and Accountability Act (HIPAA) or something else.

verizonenterprise.com/paymentsecurity

Compliant ≠ secure

Even when regulation is up to date, compliance is no guarantee of security. Most compliance assessments only audit a small subset of devices and processes. And even when processes are strong, no audit can verify that they will be followed every time or truly probe their robustness and resilience. Things change and if security controls are not monitored and fine-tuned, they can become ineffective.

Likewise, employees can be a weak link. Even when the right guidelines are in place, there is a significant risk that employees will not follow procedures and will indulge in risky behavior, such as using free Wi-Fi – whether inadvertently or deliberately.

Putting in place the right systems and then regularly assessing their effectiveness is key to improving security. Our Baseline, Better, Best matrix (see page 23) offers a starting point for defenses we think that you should have in place, and what measures you should be taking on an ongoing basis to keep your defenses in peak condition.

What the industry is doing.

Standards bodies, service providers, hardware manufacturers, device makers and academics have been working together to develop mobile standards that not just meet users' growing performance demands, but offer greater security too.

Modern cellular networks are significantly more secure than those of a few years ago, but the industry is working on making them even more robust and resilient.

4G LTE

Verizon launched its 4G LTE network in late 2010. This was a substantial step forward from existing 2G and 3G networks. Not only did 4G LTE offer significantly increased performance, it added several security improvements, including enhanced encryption, stronger authentication and better integrity protection.

> 90% of Verizon's wireless traffic now travels over our 4G LTE network[44].

Airlink encryption
4G LTE encrypts both data and signaling, separates encryption keys for specific purposes, includes backward and forward security for keys at handovers, and uses secure algorithm negotiation. This makes eavesdropping and modification attacks much more difficult.

Mutual authentication
In LTE networks, the network authenticates the user identity, while the user equipment authenticates the network credentials. Mutual authentication protects against attacks from rogue base stations, and hence, defeats man-in-the-middle attacks.

Integrity protection
Cybercriminals were able to exploit weaknesses in the signaling protocols – how devices and cell towers establish and manage connections – of early cellular standards. With advances in cellular network technology, integrity protection is used to verify that the signaling has not been modified and that the origin of signaling data is the one claimed. Each signaling message is appended with an integrity tag and the message is accepted only upon verification of the integrity by the receiving end.

5G

Much has changed since the launch of 4G LTE, both in terms of technology and customer expectations. When Verizon launched its 4G LTE network, around 60 million Americans had a smartphone[45]. Today, that number is about 260 million[46]. There are also hundreds of millions of connected devices – globally, the number using cellular connections is expected to reach 4.1 billion by 2024[47].

It's not just the volume of devices that has grown. It's now expected that you can stream video, uninterrupted and often in HD. It's not just entertainment, mobile networks are being used in mission-critical environments – including supporting first responders and connecting branch offices and remote sites.

When developing standards for 5G, the participants, including Verizon, were clear that it needed to offer an order of magnitude change in terms of performance and the number of devices that could be supported. Improved security and resilience were also high on the agenda.

While 5G standards are still being developed, there are a number of security improvements already established as part of the core design philosophy.

Greater use of virtualization and software-defined services
Cloud computing is now an established technology and software-defined networking (SDN) is quickly becoming the default choice for new fixed network deployments. So it was logical that 5G should make greater use of these technologies and be designed around service-oriented principles.

One benefit of the 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.

Less reliance on dedicated hardware and firmware also means that service providers will be able to tailor security requirements to the specific needs of different applications. 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, where privacy and resilience are less critical, could operate more lightweight security and resilience.

Another benefit of the greater use of virtualization, is that 5G network functions can be scaled more easily. As well as enabling networks to be more responsive to changes in traffic, this also means that services can be independently replaced, restarted, or isolated if they fall under attack.

Communication security
With 4G and earlier networks, security must be reconfigured on each handover between cells. 5G networks can execute sensitive functions in the central unit of the base station. This means they can reuse the same configuration across different base stations, simplifying handovers and improving security.

Under 5G, all signaling traffic is encrypted and integrity protected. User-plane traffic is also encrypted.

5G also builds on the improvements to key encryption and management in 4G. It adds additional security features like automatic recovery from malicious security algorithm mismatches, security key separation between core network functions, and fast synchronization of security contexts in both access and core networks.

Devices connecting to Verizon networks are checked against the Equipment Identity Register (EIR), and ones flagged as stolen prevented from accessing network services. This will help prevent unauthorized access and discourage device theft.

The improvements aren't just about preventing attacks, 5G is also designed to be more robust should an attack occur. It uses network slicing to segregate groups of network functions. This would enable an operator to isolate low-priority traffic, say IoT devices, on a separate slice so that it doesn't interfere with other users should a problem – such as a distributed denial of service (DDoS) attack – occur.

Trust and identity management
To support the greater volume and variety of devices, 5G supports other identifiers as well as SIMs. Additional types of credentials include certificates, pre-shared keys and token cards. This development will be particularly useful for those deploying and managing large IoT implementations.

5G also enables trust models including a vertical service provider. This could enable networks to cooperate with service providers to carry out more secure and efficient identity management for specialist applications.

Privacy
Most 4G LTE networks offer 128-bit encryption, a vast improvement on earlier standards. The time and processing power it would take to crack this means that, today, it's impractical for all but the most dedicated criminals with access to vast resources.

But computing power continues to grow and many cybercriminals have the backing of organized crime or state-affiliated operators. Attackers are also leveraging botnets – large armies of infected devices co-opted to perform tasks. While still the prevailing standard, the NSA declared that 128-bit was no longer fit for top secret communications back in 2015[48]. To keep ahead of the criminals and make it future-ready, 5G enables the use of synchronous 256-bit encryption.

5G also enables a home operator to conceal a subscriber's long-term identifier, roaming or not, while simultaneously addressing regulatory requirements. This helps prevent active attacks and makes the international mobile subscriber identity (IMSI) catchers ineffective in a 5G-only system.

Compliance/security protection
As well as defining more secure systems and protocols, 5G also covers measures to maintain secure implementation. The Network Equipment Security Assurance Scheme[49] (NESAS) is jointly defined by GSMA* and 3GPP**. It sets defined security and auditing requirements:

- The expected security controls, including the hardening of equipment and penetration testing requirements, have been defined by operators and vendors.
- The GSMA is responsible for enforcing compliance with the agreed standards. It will appoint companies to perform the audits of vendors' development and testing processes.

Verizon launched its first 5G service in four cities in late 2018. Find out more about the roll-out of additional services and new locations: verizon.com/about/our-company/5g

* The Global System for Mobile Communications Association (GSMA) is the body that represents the world's 800 mobile network operators.
** The 3rd Generation Partnership Project (3GPP) is a collaboration between telecommunications standards associations, such as the Alliance for Telecommunications Industry Solutions (ATIS) and the European Telecommunications Standards Institute (ETSI).

What companies are doing.

Not enough.

Mobile devices are prone to many of the same attacks as other devices. Most phishing attacks and badly coded sites can affect them, mobile users might even be more vulnerable. And there are also mobile-specific exploits – like malicious apps and rogue wireless hotspots.

And yet again this year, we found that many companies are failing to protect their mobile devices. And we're not talking about some almost-impossible-to-achieve gold standard. We're talking about companies failing to meet even a basic level of preparedness.

Confidence in mobile device security is lower

Figure 38. Do you agree with the statement "I'm less confident about the security of our mobile devices than other systems"?

Two thirds of organizations said they are less confident about the security of their mobile assets than other devices. A fifth (21%) strongly agreed with that statement.

This isn't surprising. As we've seen, many organizations don't have even the most basic protections in place.

Spend is going up.

As in our last report, we found that most organizations are seeing their spend on mobile security go up.

Companies said they expect mobile security spend to rise

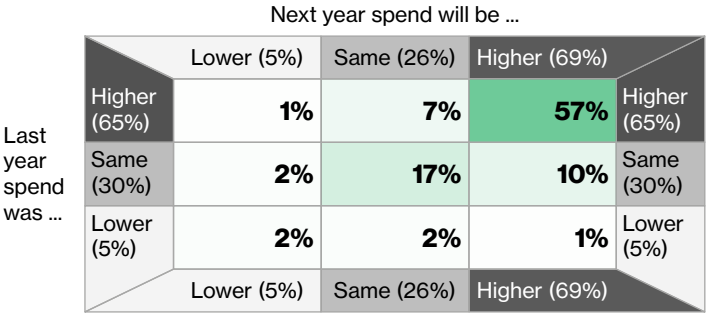


Figure 39. How has your mobile device security spend changed in the last year? And how do you expect it will change over the coming year?

Most (65%) saw their spend rise in the past year. And even more (69%) expect their spend to rise in the next 12 months. Only 24% won't have seen an increase over the two-year period.

But money's not the problem.

More thought that skills were a barrier than budget

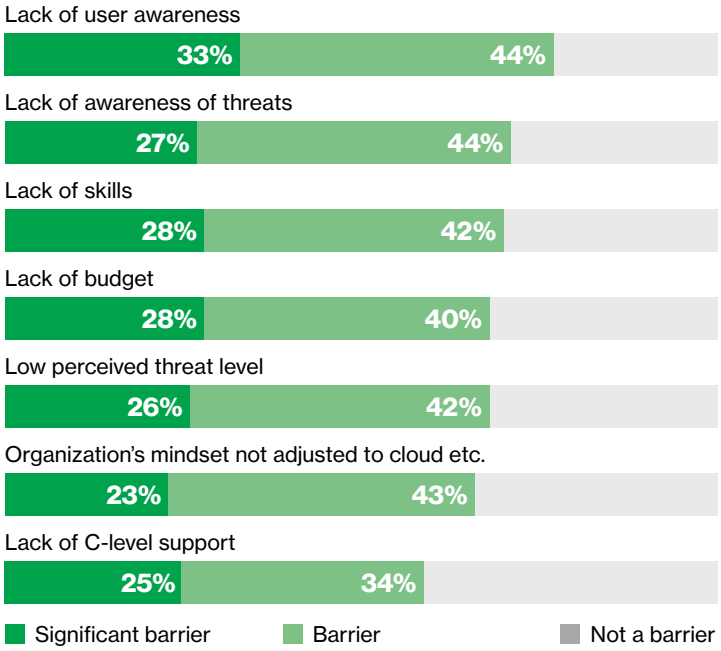


Figure 40. To what extent are the following barriers to improving your mobile device security?

As in the 2018 report, lack of C-level support came bottom of the list of barriers to improving mobile security. The top three answers offered all revolve around expertise, or lack of it.

Respondents said that their organization lacks sufficient understanding of the threats and the skills to tackle them, and their users aren't adequately prepared.

Budget was cited as a significant barrier by just 28% of respondents.

Despite their admitted lack of expertise, the majority of companies are still relying on internal resources to manage the security of their mobile devices.

How respondents' organizations secure devices

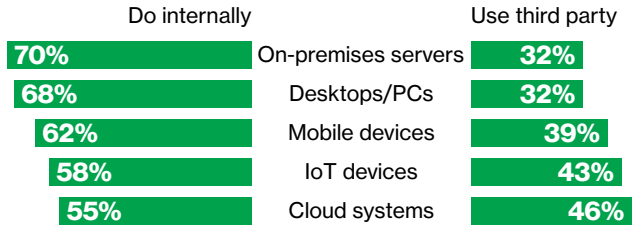


Figure 41. How do you manage the security of the following?

Companies are more likely to turn to external help to support mobile devices, but only just. As the threats increase and demand for relevant skills go up, it's questionable whether this strategy is sustainable.

Conclusion: It's time.

It could happen to you.

How did you do on the self-assessments? Our research found that most organizations remain ill-prepared for attacks on mobile devices. Are you one of them?

While some attacks are targeted, many aren't. And we found that companies of all sizes, across all kinds of industries are affected.

Organizations of all sizes were hit by mobile compromises

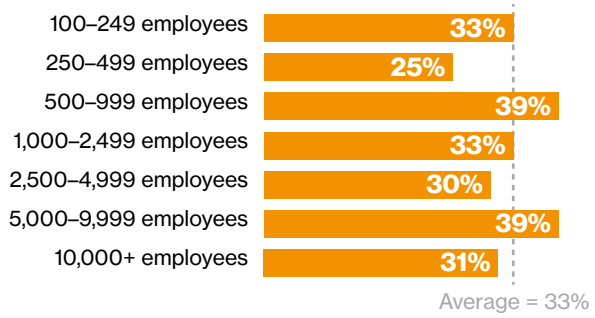


Figure 42. [Have you] experienced a security breach involving mobile devices during the past year? A breach is any security incident that resulted in the loss of data or system downtime.

While big companies have more resources (including expertise), the size and complexity of their device estate makes it harder to manage. Smaller companies have a more manageable base of devices to secure, but often lack the expertise and resources to do so effectively. The upshot: We found the likelihood of experiencing a compromise to be fairly consistent across the board.

Organizations across all sectors were affected

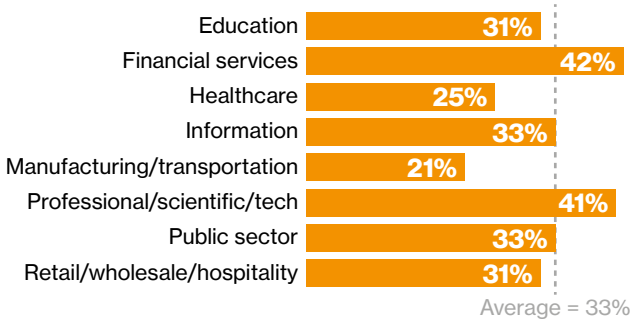


Figure 43. [Have you] experienced a security breach involving mobile devices during the past year? A breach is any security incident that resulted in the loss of data or system downtime.

Organizations aren't doing enough.

Each year for over a decade the DBIR has found that companies are taking the same gambles, and losing. Many are failing to take even basic precautions, and as a result they are exposing themselves to greater risk of downtime and massive damage to their reputation.

It's worrying that our data shows that attitudes towards protecting mobile devices are much less sophisticated than those regarding defending servers and personal computers.

They are relying on employees too much.

It's often been said that employees should be your first line of defense. There's great merit in having a well-informed workforce that can spot anomalies and provide an early warning of attacks. But our findings suggest that organizations are relying on employees in place of deploying solutions to automate and enforce security policies.

Organizations said employees are the biggest risk

Figure 44. Do you agree with the statement "Employees are the greatest risk when it comes to mobile device security"?

And partly because of this, they see employees as the greatest risk when it comes to mobile security.

Defenses like UEM and DLP could help block dangerous behavior, thwart attacks, and quickly detect and mitigate threats far more reliably than us fallible humans. And they could work out a lot cheaper than suffering a compromise.

Are you ready?

Companies need to put in place measures across the whole security cycle: assess, protect, detect and respond. And they should implement systems to enforce the rules and spot non-compliance automatically. Many companies already take this approach for other IT systems, lots more are working toward putting it in place. It's time to include mobile devices in the plan.

See our Baseline, Better, Best matrix on the next page for some suggestions on how you can get started or move up to the next level of mobile device security.

Mobile security: Baseline, Better, Best.

		Baseline	Better	Best
Assess Understand your devices, your data, who has access, and what the threats are.	Implement	• Ensure mobile is included in all your security plans and policies • Understand risk factors including geolocation, industry, size and critical data streams • Understand and manage your employees' data usage	• Take a full accounting of your assets to determine risks and potential exploits • Track updates and patches, and coordinate deployment • Define guidelines for acceptable use, including file transfer	• Measure your environment against applicable regulatory frameworks • Establish a security-first employee focus and culture • Implement a risk evaluation and scoring framework
	Maintain	• Regularly assess defenses to confirm that detection capabilities meet set standard	• Test employee mobile security awareness at least once a year	• Perform regular, at least quarterly, 360° reviews of mobile threat landscape and security posture
Protect Harden assets, protect data and secure the emerging mobile perimeter.	Implement	• Deploy a device enrollment policy • Implement a strong password policy and verify adherence • Limit Wi-Fi to approved networks • Prevent employees from installing apps downloaded from the internet • Establish formal policies for corporate-liable/BYOD detailing employees' responsibilities	• Implement a unified endpoint management (UEM) system to pre-configure devices with approved apps, limit additions to company app store and set/manage policies • Deploy a private network solution to any device that gathers or accesses sensitive data • Leverage voice, messaging and file encryption solutions	• Implement device segmentation, keeping personal and work data and applications separate • Change device procurement policies to favor cellular over Wi-Fi • Develop governance policies for the transfer of data between IoT devices
	Maintain	• Regularly review access to systems and data	• Identify users who are out of compliance or misusing assets	• Use activity-based monitoring to block malicious behavior
Detect Identify vulnerabilities and anomalies quickly to enable speedy response to reduce impact.	Implement	• Deploy mobile threat detection software to scan for vulnerabilities • Implement log monitoring to spot signs of attacks and device misuse	• Introduce a solution to identify and prevent complex phishing attacks – including those happening outside email • Implement processes to identify devices that are out of compliance	• Introduce data visibility and content control tools • Deploy secure productivity apps to protect collaboration • Implement secure IoT device visibility and management platform
	Maintain	• Provide regular security training on the dangers associated with mobile devices and how to spot warning signs of an incident	• Review apps to identify anomalies such as excessive permissions and potentially dangerous behavior like scanning corporate networks	• Use data loss prevention (DLP) tools to limit data transfer, provide early warning and enable forensics
Respond Remediate issues, recover operations and enable forensic analysis.	Implement	• Implement policies to contain attacks by locking down private information and isolating infected, lost or stolen devices	• Create an incident response plan that informs employees of what to do in the event of an incident • Implement push messaging to tell users and admins what to do in the event of an incident	• Automate corrective actions to reduce response time and limit exposure • Implement employee-friendly policies and solutions tailored to BYOD security
	Maintain	• Remind employees how to report any suspicious activity – make it an easy-to-remember email address or phone number	• Exploit the complete range of UEM capabilities to identify the full range of threats and trigger responses	• Run regular response exercises on areas of concern (e.g., phishing)

Appendices

Appendix A:

About this research.

Verizon is committed to sharing analysis, insights and best practices with the industry, government and businesses in the interest of improving the security of devices, data and critical infrastructure.

We contracted an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices. This included tablets, laptops enabled with cellular or Wi-Fi connectivity, and connected devices as well as mobile phones. Unless stated otherwise, all data in this report is from that survey.

Demographics of survey respondents

Split of respondents by industry

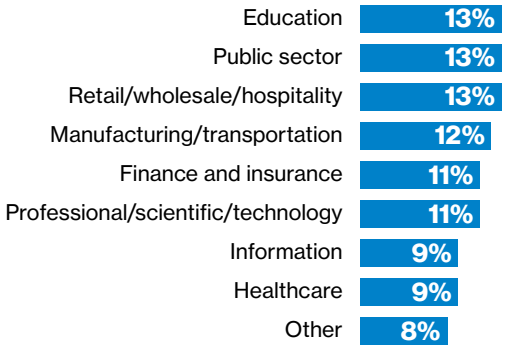


Figure 45. Which industry sector do you work in?

Our sample includes 671 respondents covering a wide range of industry sectors.

Split of respondents by role

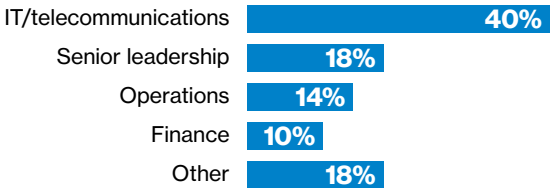


Figure 46. Which of the following best describes your current job role?

Two of five (40%) respondents described themselves as working with the IT or telecommunications function. Nearly a fifth (18%) were part of the organization's senior leadership.

The survey covered a wide range of company sizes, based on the number of employees and number of mobile devices in use.

All respondents were from the US, but many represented multi-national or global companies.

Split of respondents by company size (number of employees)

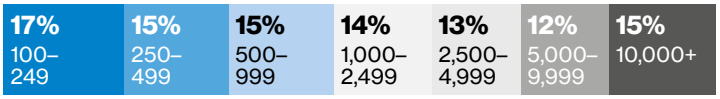


Figure 47. How many employees does your organization have?

Our sample included both small companies and large enterprises. Company size was not a strong indicator for most of our questions.

Split of respondents by number of devices

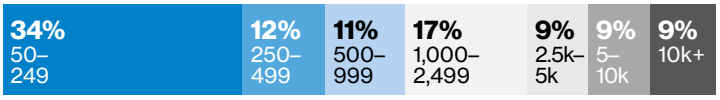


Figure 48. Approximately how many mobile devices are your employees using for work purposes? Include any device that uses cellular or Wi-Fi data (e.g. cellphone, tablet, laptop etc.).

Split of respondents by mobile OS used

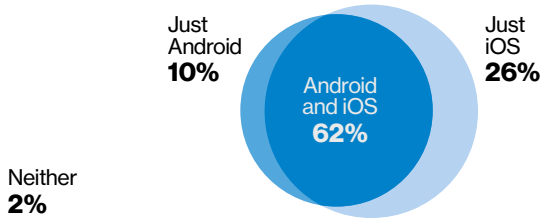


Figure 49. Which OSs do your organization's mobile phones and tablets run?

Almost all our respondents had more than one type of device in use. And the majority were using more than one mobile OS. 62% were using a mix of Android and iOS. Of those using both, 40% said most devices were Android and 41% said most devices were iOS.

How respondents' organizations procure/manage devices

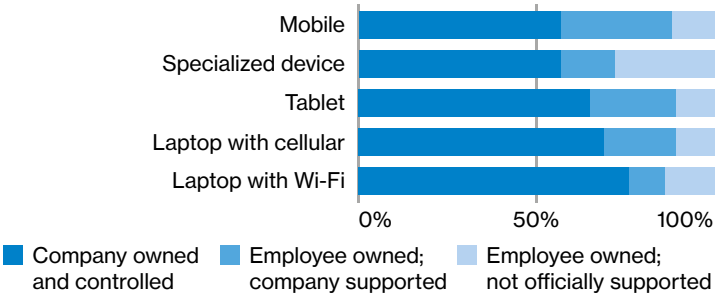


Figure 50. How are your employees provided with the following devices for work purposes?

Respondents were using multiple approaches to procuring and managing devices.

Appendix B:

Industry insights

Education

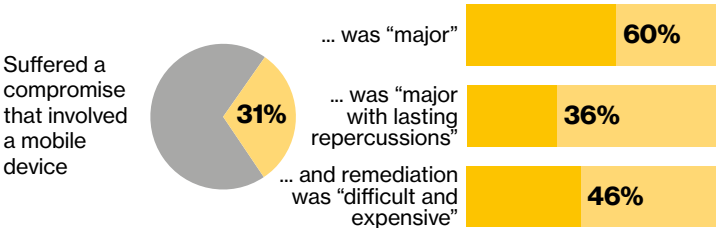


Figure 51. Breakdown of key stats for education organizations.

Cybercriminals' targets vary as much as education organizations. Verizon's 2018 DBIR found that espionage remained a significant motivation, but even if not involved in highly secretive or potentially lucrative research, educators are not off the hook. Many schools and colleges were targeted with the "W-2 scam" – this involves the theft of personal staff information, which is then used to commit identity fraud or further social engineering.

Companies in the education sector performed worst at our "four key protections" test. Just 6% had all four measures in place, compared to 12% across all industries.

Financial services

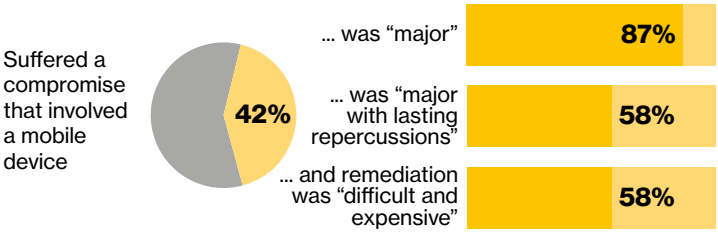


Figure 52. Breakdown of key stats for financial services companies.

90% of financial services companies said that they'd made changes to their security policies in light of new regulation.

Financial services companies were most likely to say they'd experienced a mobile-related compromise. Their close connection with money makes them an appealing target. But we shouldn't forget the other side of the coin – maybe financial services companies are just better at identifying when a mobile device was involved. They are much more likely to have some defenses in place, like DLP (46% versus an average of 36%).

But they are also much more likely to say that they'd suffered a "major" compromise. So it's little surprise that they topped the list of sectors agreeing with the statement that "organizations need to take mobile device security more seriously" – 44% strongly agreed, versus 33% across all industries.

Healthcare

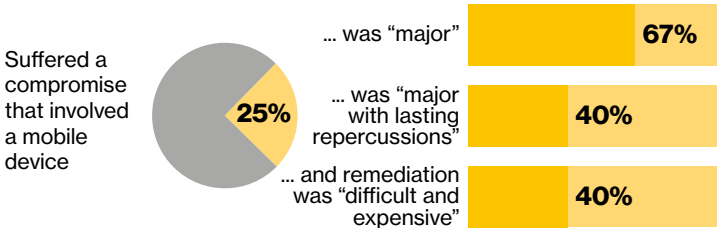


Figure 53. Breakdown of key stats for healthcare organizations.

Healthcare organizations often have many staff, many devices, and lots of potentially valuable information – not just sensitive clinical data, but also things like payment card information.

Yet, just a quarter of healthcare organizations said that they'd experienced a mobile-related compromise. That seems quite low considering how much has been published about them being a prime target for cybercriminals. It could be that they genuinely suffered fewer compromises that featured a mobile device; or maybe they just weren't as good at identifying when one was involved.

Compared to the all-industry average, healthcare organizations were much more likely to have been notified of a breach by a customer or partner – 53% versus 38%.

Information

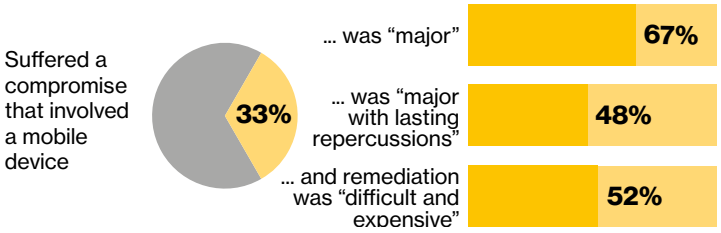


Figure 54. Breakdown of key stats for information companies.

It might be tempting to think that organizations classified as "information," which includes telecoms and data processing companies, would be the most prepared when it comes to mobile security. But of course, many of them also have more systems that they rely on, and more data at risk.

Companies in the information space were least likely to have a policy of changing all default/vendor-supplied passwords – 29% versus 39%. Information companies were the most likely to be concerned about convenience as a motive – 44% versus an average of 32%. They were also the most likely to be concerned about espionage at 29%.

Manufacturing and transportation

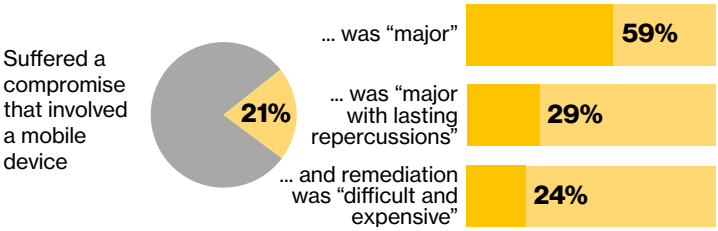


Figure 55. Breakdown of key stats for manufacturing and transportation.

The 2018 DBIR found that nearly a third (31%) of data breaches affecting manufacturers were connected to cyberespionage[50]. But in our survey, only 27% said that they are concerned about this motive. More than two thirds (68%) were concerned about employees, and just a fifth (20%) with state-affiliated actors.

Despite the relatively low proportion that had experienced a mobile-related compromise, manufacturers were very concerned about cybercriminals targeting their data. They topped the list of most concerned about many data types, including employee data, customer data, bank account details and payment card information.

Companies in this industry were nearly twice as likely to say that IoT devices had been affected as part of a compromise – 70% versus 36% across all industries. They were one of the least likely to think that their IoT security is "very effective" – just 24%, second only to the public sector at 18%.

Professional services

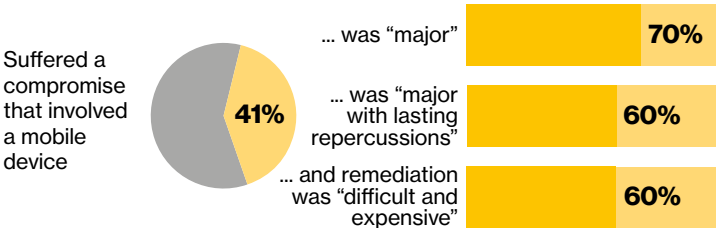


Figure 56. Breakdown of key stats for professional services companies.

Professional services companies were most likely to say that an incident had led to downtime – 80% versus an average of 64%.

These organizations were the most likely to be concerned about cybercriminals targeting intellectual property – nearly a half (47%) compared to an all-industry average of 34%.

Companies in this industry were most likely to be "very confident" in their ability to spot a compromised device (47%) or an employee misusing a device (51%) quickly. But they were also most likely to have found remediating a compromise "difficult and expensive" – 60% compared to an average of 43%.

Professional services companies were most likely to be "very concerned" about the volume of mobile data being used.

Public sector

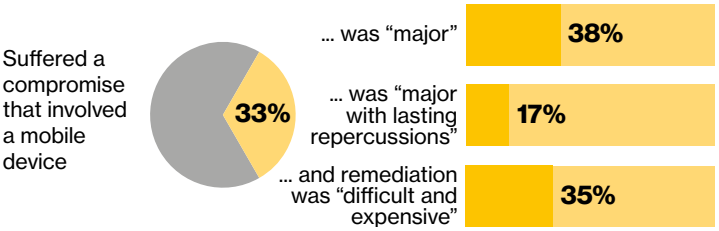


Figure 57. Breakdown of key stats for public sector organizations.

Public sector organizations were least confident in the knowledge of their employees. Just one in eight (12%) of respondents said that their colleagues are highly knowledgeable, compared with 27% across all industries.

The theft of authentication credentials is a worry in the public sector. 53% of organizations said they are concerned about these being compromised due to ineffective mobile security. Across all industries that figure was just 40%.

Organizations in this sector were least likely to say that they'd sacrificed mobile device security for expediency or business performance – 30% compared to an average of 48%.

Retail, wholesale and hospitality

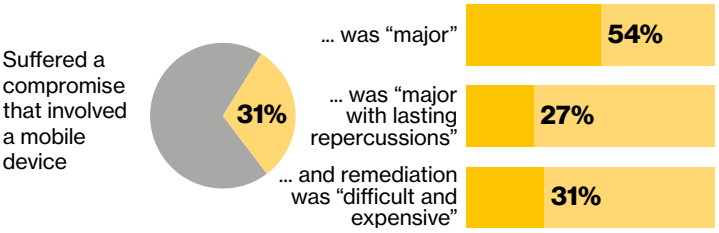


Figure 58. Breakdown of key stats for retail, wholesale and hospitality companies.

Many retail companies have to comply with PCI DSS. This regulation provides a solid framework for building strong security policies and procedures. But our annual Payment Security Report[51] has found that many companies struggle to maintain compliance between annual assessments.

Retailers were most likely (55% versus an average of 37%) to be concerned about cybercriminals stealing payment card details. Not really a surprise. But they were also more likely to be concerned about customer data being taken (61%).

Of the companies in this sector that had suffered a compromise, two thirds (67%) were notified by a third party such as a customer, a partner or law enforcement.

For more industry-specific insight, see our snapshots for financial services, healthcare, manufacturing, public sector, retail, plus small businesses: Read our snapshots

Appendix C:

Contributors

IBM MaaS360 | With Watson

For IT and security leaders who are responsible for managing and securing smartphones, tablets, laptops, desktops, wearables and IoT across their organization, IBM MaaS360 with Watson is the only platform that delivers a cognitive/artificial intelligence (AI) approach to unified endpoint management (UEM) to enable endpoints, end users and everything in between – including apps, content and data.

Delivered from a world-class cloud, MaaS360 is recognized for its fast, simple, and flexible deployment model. Offering an open platform, MaaS360 makes integration with existing apps and systems seamless and straightforward.

IBM contributions:
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. We are trusted by hundreds of millions of individual users, enterprises and government agencies and partners such as Verizon, Microsoft and Apple.

Powered by the largest dataset of mobile code in existence, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk. The installed base of our 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 contributions:
We leveraged our mobile dataset, the world's largest, to provide data used in this report. We also collaborated with Verizon to analyze the results and provide insight on the current threat landscape.

lookout.com

MobileIron

MobileIron, the secure foundation for modern work, provides cloud and endpoint security so employees can make better, faster decisions using cloud services and mobile experiences. MobileIron is both a 2018 Gartner Magic Quadrant Leader and a 2018 Gartner Peer Insights Customers' Choice for Unified Endpoint Management.

MobileIron contributions:
Unless otherwise specified, MobileIron data is from devices with threat detection activated across the installed base of MobileIron Threat Defense and Zimperium.

mobileiron.com

wandera

Wandera is the experts' choice in mobile security. Recognized by leading analysts for its capabilities in mobile threat defense, Wandera's Secure Mobile Gateway provides extensive risk management across mobile endpoint, network and applications.

With the industry's largest mobile dataset coupled with real-time analytics through its MIRIAM intelligence engine, Wandera is the only solution that gives mobility leaders the visibility and control they need to effectively manage their mobile data.

Founded in 2012, Wandera's award-winning technology protects over one thousand global enterprise customers who collectively manage 2+ million mobile devices. Wandera is headquartered in London and San Francisco.

Wandera contributions:
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

About Verizon

Verizon is a global leader in technological innovation, from mobility and networking to business communications. Our 4G LTE network is the largest in the US, and it's now available in more than 500 markets from coast to coast.

We have over 25 years of industry experience, nine Security Operations Centers, six forensics labs and one of the largest IP networks in the world. We monitor 61 billion security events (on average) each year to improve our threat library and inform our teams. Our world-class services and security professionals, are always ready to help you meet your security challenges.

We're the only provider recognized by industry analyst firm Gartner as a leader in both Network Services and Managed Security Services in its 2018 Gartner Magic Quadrant reports.

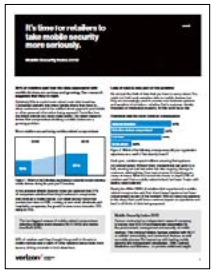
We're also leading by example. Our business operates under a rigorous information security policy, and we maintain physical, technical, and administrative safeguards for our systems.

We take a layered approach and create flexible security strategies, which we can adapt and scale to match your organization's growth and requirements. Trust us to protect your network in the same way we protect our own, around the clock and around the world.

More on mobile security.

Executive Summary
An abridged version of this report written for those outside the IT/security department. It can help make the case for reviewing mobile security with leaders and executives from other functions.

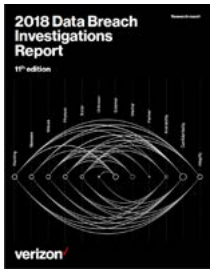
Read our summary >



Industry snapshots
Detailed insights into the state of mobile security in finance, healthcare, public sector, manufacturing, and retail organizations, as well as at small companies (up to 499 employees).

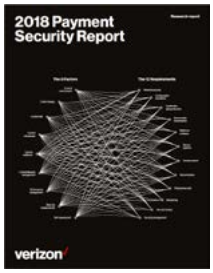
Read our snapshots >

Other Verizon security publications.



Data Breach Investigations Report
For over a decade, Verizon's Data Breach Investigations Report (DBIR) has been one of the IT industry's most respected security publications. It's based on analysis of thousands of confirmed data breaches and tens of thousands of security incidents.

Download the latest edition >



Payment Security Report
Almost half (47.5%) of organizations that achieve PCI DSS compliance fail to sustain it until their next annual assessment. Read the Payment Security Report to discover which controls they failed to maintain, and how you can avoid the same fate.

Download the latest edition >

We offer world-class products to secure mobile devices, content, and applications. With Verizon, you can choose the most effective security solution for your business needs.

Learn more >

References

1. MobileIron, Global Threat Report, mid-year 2018
2. MobileIron, Global Threat Report, mid-year 2018, based on analysis of privacy and security settings like whether a device has “developer options” enabled, is jailbroken or rooted, has necessary security settings like encryption and PIN codes disabled, has code signing deactivated, has apps from unknown sources or harbors malicious profiles.
3. Verizon, Data Breach Investigations Reports, 2009-2018, https://enterprise.verizon.com/resources/reports/dbir/
4. Lookout analysis of data aggregated from its 70M+ corpus of apps and 170M+ users of its mobile endpoint products between October 2017 and October 2018.
5. Wired, How to Protect Yourself From the Giant Marriott Hack, November 2018, https://www.wired.com/story/marriott-hack-protect-yourself/
6. Wandera customer example.
7. Wandera Mobile Data Research. Investigation of mobile usage trends across a global customer base. Study covered one full year (November 2017 to October 2018) of real-world mobile device usage across all represented. verticals and geographic regions.
8. Lookout analysis of data aggregated from the 170 million+ users of its mobile endpoint products between October 2017 and October 2018.
9. Lookout analysis of data aggregated from the 170 million+ users of its mobile endpoint products between October 2017 and October 2018.
10. Wandera Mobile Threat Research, What are app permissions - a look into Android app permissions, February 2018, https://www.wandera.com/mobile-security/app-and-data-leaks/app-permissions/
11. Incident data on L33bo phishing kit provided by Lookout, 2018.
12. Findings by Lookout between October 2017 and October 2018.
13. Wandera Mobile Threat Research, Mobile phishing report, May 2018
14. Findings by Lookout between October 2017 and October 2018.
15. FBI, Latest Internet Crime Report Released, May 2018, https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718
16. Findings by Lookout between October 2017 and October 2018.
17. MobileIron, Global Threat Report, mid-year 2018. Period covered was first half of 2018.
18. Data from Wandera Mobile Threat Research.
19. Wandera Mobile Threat Research, What is punycode? Fake domains that deceive the human eye, November 2018, https://www.wandera.com/mobile-security/phishing/punycode-attacks/
20. Trial data from Wandera Mobile Threat Research. Test conducted over a one-year period (November 2017 to October 2018). Based on organizations testing a mobile security solution with real end users.
21. Verizon, 2018 Data Breach Investigations Report, 2018, https://enterprise.verizon.com/resources/reports/dbir/
22. Wandera, Beware iOS users: malware is by no means an Android-only problem, November 2017, https://www.wandera.com/beware-ios-malware/
23. Aggregated metrics from IBM MaaS360 Mobile Metrics benchmarking data, generated from global IBM MaaS360 client implementations.
24. OWASP, Mobile Top 10 2016-Top 10 , 2016, https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
25. Researchers from Wandera Mobile Threat Research ran a series of experiments using two similarly configured mobile devices (same operating system, same settings and same starting battery health) to test the impact of cryptojacking across two scenarios. In one scenario, the device loaded a webpage configured with a cryptojacking script, while in the second scenario, the device did not. Both scenarios were run multiple times using fresh devices and the median values reported. In all experiments, device screens were configured at full brightness and active web surfing was simulated.
26. Over a one-year period (November 2017 to October 2018) Wandera Mobile Threat Research identified that 25% of organizations within their mobile-enabled user base experienced a mobile cryptojacking incident. Cryptojacking scripts were observed in web pages, mobile ads and in connected mobile apps.
27. Kensington, Cost of stolen or lost laptops, tablets and smartphones, 2012, https://web.archive.org/web/20121224201300/http://blog.kensington.com:80/wp-content/ktg/docs/m1_iphone_theft_banner.pdf
28. Analysis of common configuration vulnerabilities by Wandera Mobile Threat Research. Covered enterprise mobile devices in production environments during a one-year period (November 2017 to October 2018).
29. Aggregated metrics from IBM MaaS360 Mobile Metrics benchmarking data, generated from global IBM MaaS360 client implementations.
30. Distribution data and mapping to CVEs provided by Wandera. Researchers from Wandera Mobile Threat Research analyzed vulnerability information that has been published for each mobile platform in use by global organizations to assess the risk associated with each out-of-date operating system. The findings covered both minor and major OS updates.
31. Aggregated metrics from IBM MaaS360 Mobile Metrics benchmarking data, generated from global IBM MaaS360 client implementations.
32. MobileIron analysis of published CVE data.
33. Aggregated metrics from IBM MaaS360 Mobile Metrics benchmarking data, generated from global IBM MaaS360 client implementations
34. Lookout, The Spectrum of Mobile Risk: Understanding the full range of risks to enterprise data from mobility, 2017
35. Wandera Mobile Threat Research, Mobile Wi-Fi Security Report, 2018
36. Ibid.
37. MobileIron, MobileIron Global Threat Report Mid-Year 2018, 2018
38. Investigation into the security of Wi-Fi networks by Wandera Mobile Threat Research. The type of encryption used (or not used) on the wireless channel of access points around the world was analyzed, November 2018.
39. Analysis of public Wi-Fi networks by Wandera Mobile Threat Research. based on the networks encountered by mobile devices running the Wandera mobile threat defense app during November 2018.
40. MobileIron, Global Threat Report, mid-year 2018
41. California State Legislature, SB-327 Information privacy: connected devices, 2018, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
42. Infosec Magazine, Superdrug Held to Ransom After Breach, August 2018 https://www.infosecurity-magazine.com/news/superdrug-held-to-ransom-after/
43. Bank Info Security, Air Canada: Attack Exposed 20,000 Mobile App Users' Data, August 2018, https://www.bankinfosecurity.com/air-canada-attack-exposed-data-on-20000-mobile-app-users-a-11441
44. Verizon, 2019, https://www.verizon.com/about/our-company/wireless-network
45. Comscore, December 2010 US Mobile Subscriber Market Share, 2011, https://www.comscore.com/Insights/Press-Releases/2011/2/comScore-Reports-December-2010-US-Mobile-Subscriber-Market-Share
46. Deloitte, 2017 Global Mobile Consumer Survey: US edition, 2017, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf
47. Ericsson, Mobility Report, November 2018, https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf
48. National Security Agency, Cryptography Today, August 2015, https://web.archive.org/web/20160120060933/https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
49. GMSA, Network Equipment Security Assurance Scheme, https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme
50. Verizon, 2018 Data Breach Investigations Report, April 2018, https://enterprise.verizon.com/resources/reports/dbir
51. Verizon, 2018 Payment Security Report, September 2018, https://enterprise.verizon.com/resources/reports/payment-security/2018/

verizon business ready