Mobile Security Index 2018

An in-depth look at the risks and what you can do about them.

verizon

Foreword

Organizations are increasingly hooked on mobile. Pervasive, affordable mobile connectivity is behind many of today's big changes – like digital transformation and the Internet of Things (IoT) – that are impacting processes and people across all industries.

We are also doing more and more with mobile devices. And the increased use of cloud computing and web apps is allowing many users to access vast amounts of data on these devices, helping them work better and faster.

But it's not all good news. Our experience shows that many organizations aren't fully prepared for the security challenges caused by the increased use of mobile connectivity and devices – and the increased access to information.

We wanted to know more about what organizations fear and what security measures they are taking to mitigate risks. To find out, we commissioned independent research, surveying more than 600 mobility professionals. The results were eye-opening.

Nothing is 100% secure, the challenge for those responsible for IT security is to reduce risk to an acceptable level. But our research found that approximately one third of organizations have knowingly sacrificed security for expediency or business performance. Think about that. One in three organizations that we work with, buy from, turn to for healthcare, and that govern the communities in which we live, have put speed and profit before the safety of their data – and our data. And that's just the ones that are aware and willing to admit it. The number could be significantly higher.

According to our research, many companies haven't taken even the most basic precautions to protect their data and core systems. This is alarming since the danger of cyberattacks continues to grow. Many factors make mobile devices an appealing target: there are more of them (including IoT devices), they have access to more data, and they are now critical to business operations.

There's considerable cause for concern. Yet, organizations can take simple actions to significantly protect their operations, data and reputation. In this report, we have included recommendations that can help you strengthen your organization's mobile security. We offer a flexible framework that includes security measures for your network, devices, apps and people. In short, we provide steps that you can take today for a more secure tomorrow.

Thomas T.J. Fox

Senior Vice President
Wireless Business Group
Verizon

Verizon is one of the largest network providers in the world. Our global Network Operations Centers and Security Operations Centers process more than one million security events every day, so we understand the rapidly changing nature of cyber threats. We're the only provider recognized by industry analyst firm Gartner as a leader in both Network Services and Managed Security Services in its 2017 Gartner Magic Quadrant reports.

To find out more, see page 21 or visit:

verizonenterprise.com/products/security

Contents

To produce this report, Verizon commissioned an independent research company to survey over 600 professionals involved in procuring and managing mobile devices for their organizations.

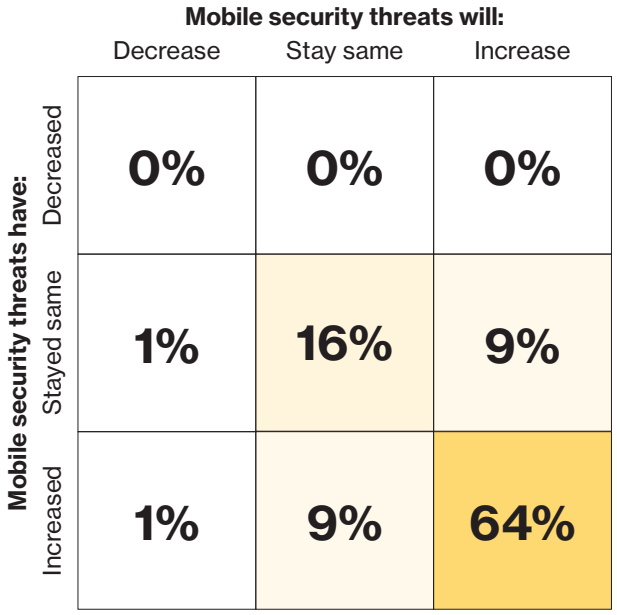
The organizations represent multiple industries and sizes, ranging from as few as 250 employees to more than 10,000. For more on the methodology behind this report, see page 20.

Executive summary

Organizations say that mobile security risks are increasing.

Companies are concerned about the threats mobile devices pose to both their data and uninterrupted business operations. While the number of reported incidents is still relatively low, the vast majority think that the threat is serious:

- 85% said their businesses face at least a moderate risk from mobile security threats. 26% said it is a significant risk.
- 74% said that the risks associated with mobile devices have increased in the past year. Just 1% said they had gone down.
- 73% said that they expect risks to increase during the next year. Only 2% said that they expect them to decrease.



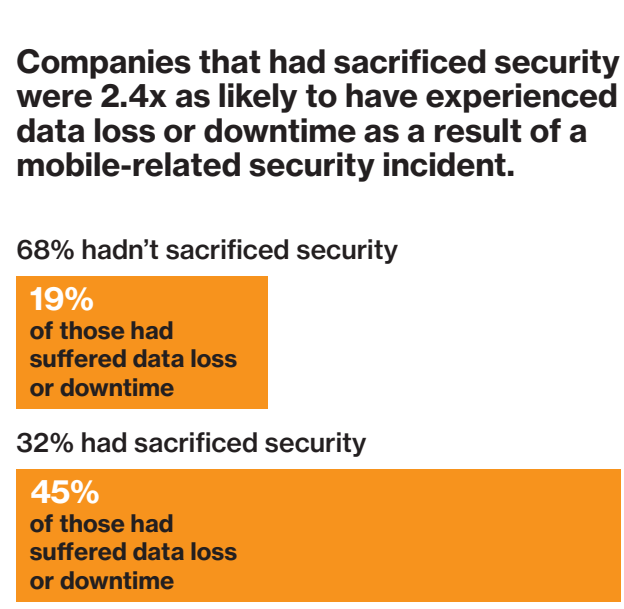
Most companies said mobile security threats increased in the last year, and will increase again in the coming year.

Share Tweet

Despite this, they are sacrificing security for expediency.

Organizations are knowingly putting speed and profits before mobile security. And the consequences are not surprising:

- Almost a third (32%) admitted to having sacrificed mobile security to improve expediency and/or business performance – 38% of those said that their organization is at significant risk from mobile threats.
- Over a quarter (27%) said that during the past year their company had experienced a security incident resulting in data loss or system downtime where mobile devices played a key role. An additional 8% said that while they hadn't, one of their suppliers had.



32% of companies sacrificed mobile security for expediency. They were 2.4x as likely to suffer data loss or downtime.

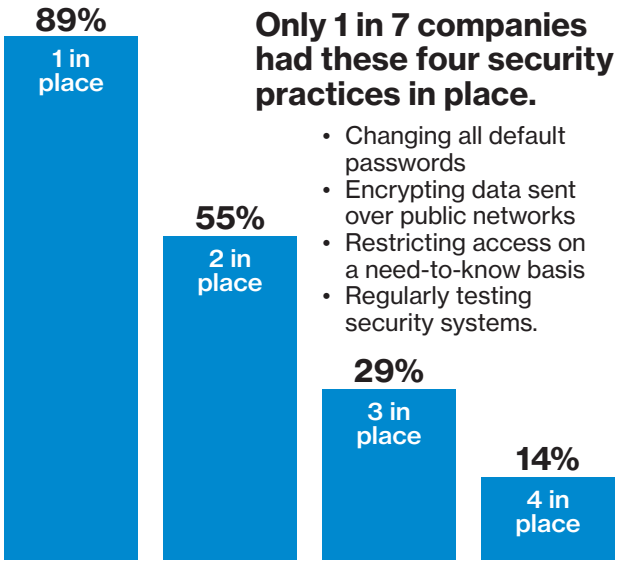
Share Tweet

Organizations are failing to take basic precautions.

It has repeatedly been found that basic security failings are behind the majority of breaches. Despite this, we found that many companies do not have some of the most basic mitigation measures in place:

- Less than two fifths (39%) change all default passwords.
- Only 38% use strong/two-factor authentication on their mobile devices.
- Less than half (49%) have a policy regarding the use of public Wi-Fi, and even fewer (47%) encrypt the transmission of sensitive data across open, public networks.
- Only 59% restrict which apps employees download from the internet to their mobile devices.

The Verizon Data Breach Investigations Report (DBIR) has been reporting on the factors behind real-world data breaches for 10 years.



Just 14% of companies had all four basic mobile security measures in place.

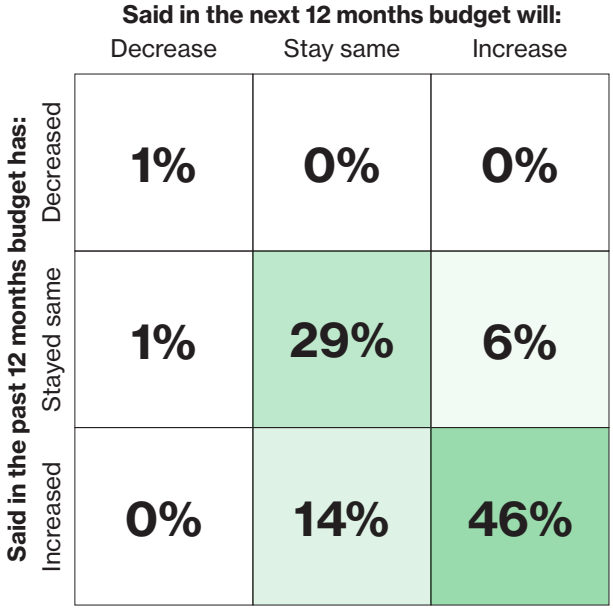
Share Tweet

But there's a consensus on the need to take more action.

It's not surprising that almost all respondents (93%) think that organizations should be taking mobile security more seriously:

- 93% said mobile devices present a serious and growing threat.
- 83% agreed that organizations are complacent about mobile security, and 24% of those strongly agreed.
- 79% said disruption of systems is an even greater threat than the theft of data – those using IoT were particularly concerned.
- 61% said that their spend on mobile security had increased in the past year. 10% said it had increased significantly.

Now is the time to get ahead of the potential dangers and make sure that your business is protected.



46% of companies said their mobile security budget increased last year and will again next year.

Share Tweet

How big is the problem?

We found that over a quarter of organizations had suffered a mobile security incident that had resulted in data loss or downtime in the last year. Many were described as "major, with lasting repercussions."

We're all aware of the increased role that mobile devices now play in business. This makes them an appealing target for cybercriminals. It's not just the theft of data that they hold – mobile devices pose a number of types of threat.

Basic types of mobile threats.

Denial of service	Jamming of wireless communications, overloading networks with bogus traffic, ransomware, or loss/theft of device
Geolocation	Gathering data on location, infringing on the privacy of the individual
Information disclosure	Interception of data in transit, leakage or exfiltration of user, app or enterprise data, eavesdropping on voice or data communications, surreptitiously activating the phone's microphone or camera to spy on the user
Spoofing	Email or text message (SMS) pretending to be from boss or colleague, fraudulent Wi-Fi access point or cellular base station mimicking a legitimate one
Tampering	Modifying data in transit, inserting tampered hardware or software into supply chain, repackaging legitimate app with malware, modifying network or device configuration (such as "jailbreaking" or "rooting" a phone)

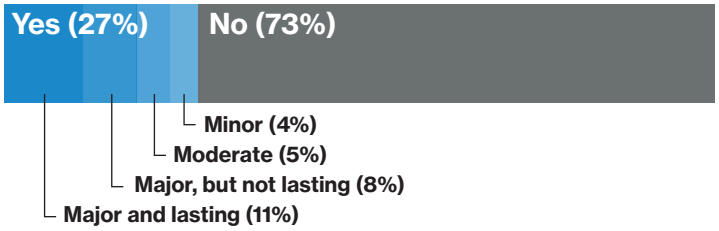
Source: Types of mobile threat, adapted from the Department of Homeland Security Study on Mobile Security, April 2017

How common are incidents?

We asked respondents if they had experienced a security incident that was directly attributable to a mobile device; and, if so, how significant was the event.

Over a quarter (27%) admitted to having experienced an incident that resulted in data loss or system downtime during the past year. And 40% of those (11% of the total) said that the incident – or the most serious one if they had experienced multiple – had been major with lasting repercussions.

Have you experienced a security incident directly attributable to a mobile device in the past year?



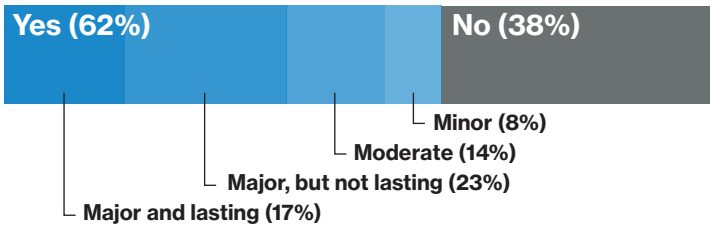
Bigger companies, those with 1,000 or more employees, were more likely to have suffered an incident – or at least knew that they had suffered an incident and were willing to admit it.

When we extended the question to include customers, suppliers and competitors, over three fifths (62%) said that one of these groups had suffered downtime or data loss. And over half of those said that the incident had been a major one.

35%

Healthcare organizations were hit hard. Over a third said they had suffered data loss or downtime due to a mobile device security incident. See page 18 for more industry insight.

Have you, a customer, a supplier or a competitor experienced a security incident directly attributable to a mobile device in the past year?



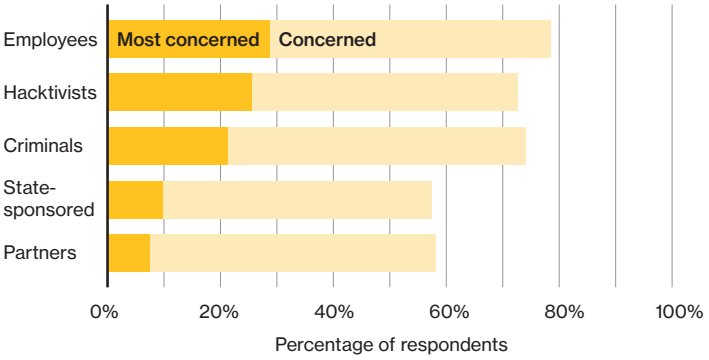
Who, what, how and why?

We asked respondents about which threats they were aware of, concerned about and had experienced. Malware, ransomware and device theft/loss emerged as the top threats that companies are concerned about and are most likely to cause incidents.

Who are companies concerned about?

While our respondents expressed concern about professional criminals and hacktivists, they were even more worried about threats originating from within their own organization. 79% said that they considered their own employees a significant threat.

Which of the following actors are you concerned about?



And it's not just negligence – such as losing devices, making careless errors or circumventing security policies – that is causing concern. Over half (58%) of respondents fear employees will do something bad for financial or personal gain.

Employees, and ex-employees, might – either maliciously or unknowingly – expose organizations to risk in many ways: accessing work resources over insecure networks (like public Wi-Fi), downloading unapproved apps from the internet, failing to set access restrictions, using weak passwords, or even something as simple as not setting a lock-screen PIN.

To maintain security, employees should only have access to sensitive information on a "need to know" basis. But over time, an employee may hold many different roles within an organization – and it's not unusual for companies to forget to adjust access rights accordingly. Access rights may not even be revoked when an employee leaves.

Loss or theft of devices is also an ever-present problem. Worldwide, tens of millions of devices go missing each year. It's not just the data stored on the device that you need to worry about, the device could also give access to even more critical data and systems.

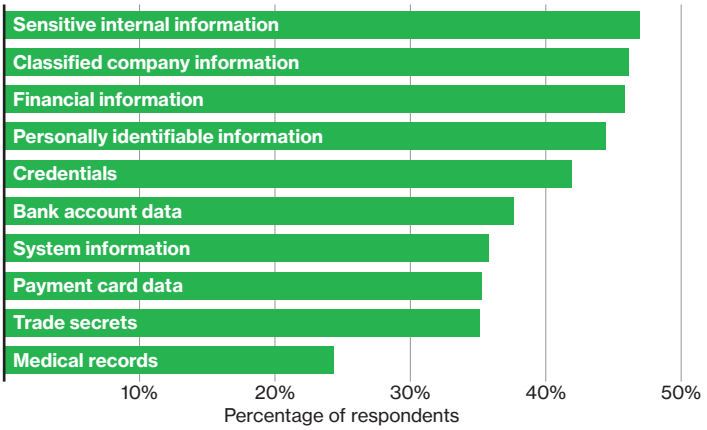
25%

of respondents in a survey by Kensington said they had experienced IT theft from planes, cars and trains; and 23% from the office[2].

What do companies think are targets?

Most cyberattacks are opportunistic. Cybercriminals are often not particular about who or what they target – as long as they can make money from it. Credentials and personal information are appealing as they can be used to commit identity fraud or gain access to accounts on other systems. And, of course, payment card data and bank account information can give a direct route to money.

Which types of data are you concerned about?



It's encouraging that many companies outside the healthcare industry recognized the risk associated with personal medical data. Any company that holds health-related data – and many hold it as part of employee records – is responsible for keeping that data secure. And if the organization operates in the US, it may be bound by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Not all cybercriminals are trying to steal data.

We're all familiar with "information gathering" hacks where data is stolen, either to be sold, used to commit theft or fraud, or exposed. But that's not the only type of incident that you need to worry about. The recent outbreak of high-profile ransomware attacks has made more people familiar with "hold hostage" attacks, where data is rendered unusable until you pay to release it. "Manipulation" hacks, where changes are made to data, are still less well-known. These might fly below the radar of your security measures, but can have a much larger effect. Important business decisions could be made on the basis of incorrect information, and the consequences not uncovered for years. And finally, there are attacks that aren't about data at all. "Disruption" hacks seek to interfere with normal business operations.

39%

of respondents whose organizations use employee-owned devices ranked them as their #1 concern. 76% ranked them in their top three.

While bring your own device (BYOD) policies are popular with many employees, employee-owned devices can introduce significant security risks for the organization.

Employee-owned devices topped the list of things that our respondents were most concerned about being exploited – ahead of IoT devices, custom apps and servers.

And it's not just smartphones and tablets that employees are bringing into the workplace. Over a quarter (28%) of respondents said that employee-owned laptops with either Wi-Fi or mobile data are being used in their organization.

Only 61%

of organizations said they own all mobile phones in use for work tasks (62% own all tablets). So most lack full control over mobile devices used in their organizations.

Who owns the device is of less concern than who controls it. If it's employee-controlled, the company may not be able to enforce security measures like data encryption and anti-virus protection, or ensure that patches and updates are applied. This can create serious security gaps that may be exploited by cybercriminals.

There are also other risks introduced by employees who behave differently when they "own" a device – even if the company has given them an allowance to pay for it. They may be more inclined to download apps, visit sites and use networks on what they see as a personal device – things that they wouldn't do on a corporate-owned and controlled device.

Storing personal and work data on one device can also cause security problems. For example, what happens when an employee leaves the company or transfers departments? It might be harder to "wipe" the device or revoke access.

20%

of companies that said they are using IoT devices put them at the top of their list of concerns.

Where our respondents said that their organization uses IoT devices, these caused a significant amount of concern. 20% of those surveyed said that IoT devices are their biggest concern. (See the section on IoT risks and what you can do about them on page 14.)

How are attacks being carried out?

We asked respondents about which threats they were aware of, concerned about and had experienced. Malware came top (72%) of the list of threats most likely to be the cause of a security incident, according to our respondents. Ransomware, a specific type of malware where data is encrypted and a fee demanded to unlock it, came second (64%), with device loss/theft (64%) a very close third.

Only 43% said that "weaknesses in custom apps" is on their radar. Interestingly, a high proportion (61%) of those had actually experienced a security incident caused by an app weakness. Less than one in seven of those that hadn't actually suffered the problem recognized the danger.

Just over half (53%) were concerned about rogue or insecure Wi-Fi hotspots. This is surprising given the seriousness of the risks. 7% said that they were not even aware of the dangers. See Appendix B (page 16).

Respondents said that security incidents (involving themselves, customers, suppliers and competitors) are most likely to be attributed to malware (48%). Malware was also blamed for more severe incidents than any other method (39%).

Consider that all 10 threats featured in the survey were the causes of a significant number of incidents. This spread of threats shows what a sizeable challenge securing mobile devices presents.

14%

said that they personally use public Wi-Fi for work tasks despite it being officially prohibited – and remember, our respondents were all responsible for mobile device policies.

Kracking Wi-Fi.

In late 2017, a serious vulnerability in WPA2, the encryption standard used by most Wi-Fi networks was uncovered. KRACK (Key Reinstallation AttaCK) affects the Wi-Fi protocol itself – not specific products or configurations. It makes it possible for attackers to eavesdrop on your transmissions over both public and private Wi-Fi. Device manufacturers were quick to publish updates to close this potential weakness. This highlights the importance of keeping up-to-date with OS updates and patches.

The industry is constantly working to improve the security of network protocols. A new version of WPA, WPA3, has recently been announced. And mobile standards have been evolving too. 4G LTE networks offer significant security advantages over previous mobile standards. (See page 19.)

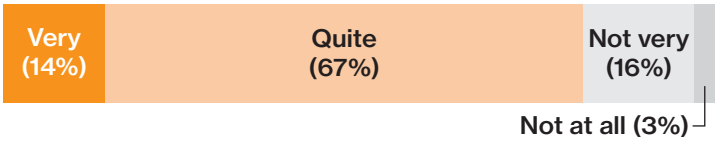
What are companies doing?

Despite broad agreement that the potential risks are serious and growing, most companies are not well prepared.

How effective are existing defenses?

Few respondents were prepared to say that their existing mobile security measures were not at all effective. But only 14% said their current degree of protection is very effective. Two thirds described their current readiness as quite effective.

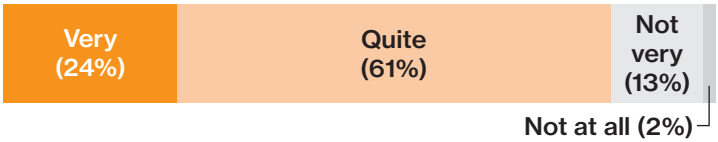
Effectiveness of existing mobile security measures.



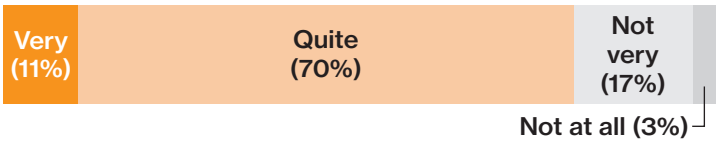
Of those who admitted that their organization had suffered a major incident, 24% said that their defenses are very effective – 13 percentage points higher than the rest. Presumably this means that they have improved their defenses in light of the incident. This is supported by the fact that 71% experiencing an incident said that their mobile security budget had increased in the past year – and 25% said that the increase was significant.

Effectiveness of existing mobile security measures.

Companies affected by data loss or downtime



Those not affected



Most companies think they're doing "OK."

Most respondents said that they thought their company's mobile security measures were somewhat effective. But only one in seven were prepared to go as far as saying they were very effective. Given that most respondents said that they think the risks are serious and growing, this suggests that most companies are unprepared for the severity of the threats that they face.

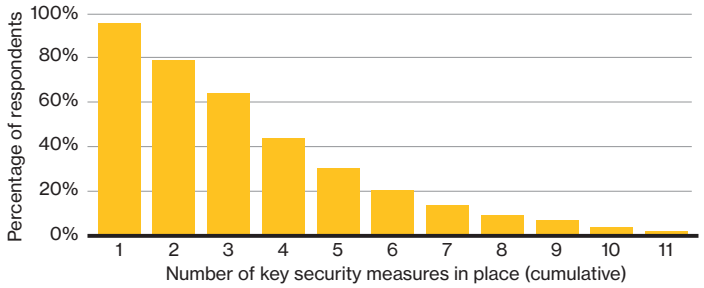
Companies are missing many of the basics.

Despite the risks, companies are not taking appropriate steps to help them manage mobile devices and people securely. This includes activating security features built into devices that don't require expensive training or incur additional costs.

- Just 47% said their organization uses device encryption.
- Fewer than one in three (33%) use mobile endpoint security.
- Only 31% of companies are using mobile device or enterprise mobility management (MDM or EMM).

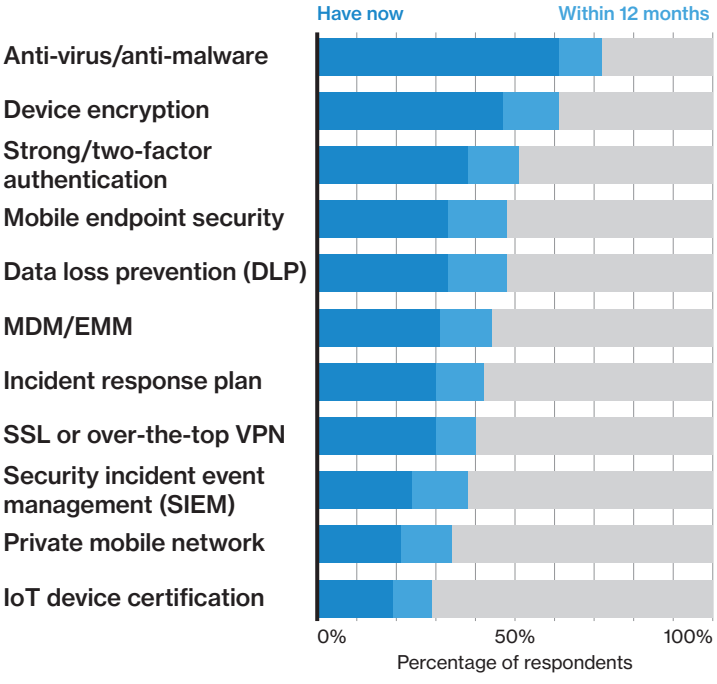
Of the 11 security measures we asked about, nearly all respondents had at least one of these measures in place, but 17% had only one and only 30% had more than four.

Key security measures in place.



Anti-virus/anti-malware was the measure most likely to be in place, but even this was only being used by 61% of companies.

Mobile security technologies in place and planned.



It's alarming that nearly two fifths (39%) of organizations are still failing to change all default passwords – one of the most basic security best practices. Research has found that poor credential management is a common thread in many breaches – the 2017 DBIR found that it factored in 81% of all hacking-related breaches. Cracking weak passwords is easy enough, but not changing default passwords makes it incredibly easy for the bad guys.

That's not the only basic security practice that many companies don't have in place:

- Over half (51%) said their organization doesn't have a policy regarding public Wi-Fi – it was neither officially sanctioned nor prohibited.
- Over half (55%) of those that don't have a policy on the use of public Wi-Fi – and so presumably didn't have safeguards in place – said they don't always encrypt sensitive data when it's transmitted across open, public networks.
- 41% said employees in their company use unscreened apps downloaded from the internet.

Many companies aren't checking devices for obvious signs of vulnerability, such as compromised OS (43%), known vulnerabilities (44%), or outdated or unpatched OS (46%).

The biggest relative growth in adoption is expected in security incident event management (SIEM) and private mobile network services. Use of these measures is expected to grow by over 50%. In terms of absolute growth, the biggest increase is expected in mobile endpoint security.

Who are companies turning to for help?

46% of respondents said that they turn to colleagues when they need help. Only 22% said that this is the only place they turn to for help. The remaining 78% said they also turn to other sources of support, including an external vendor, communications service provider, systems integrator or value-added reseller for help.

Nearly three quarters are already using a third party to provide security services. 56% are using an external vendor to provide mobile security services.

46%

of respondents said that they turn to colleagues when they need help.

Employee awareness is quite low.

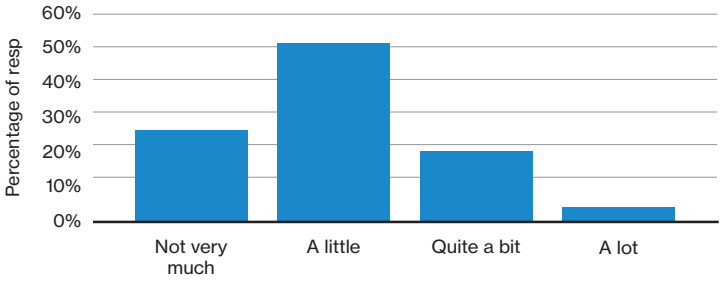
The vast majority of respondents (86%) said that their organization trains employees on mobile device security. Yet 59% of those (50% of all companies) only provide that training when the employee joins the company or is issued a new device.

Since mobile security threats and the security policies addressing these threats are constantly evolving, ongoing training has become a must in today's highly mobile world.

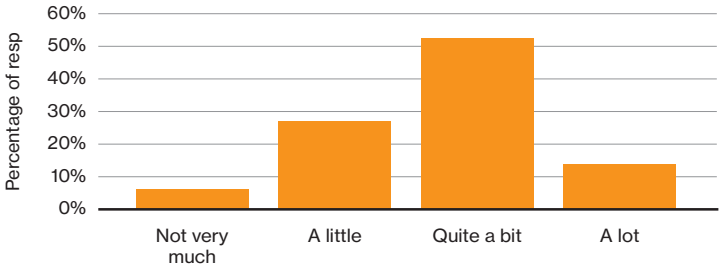
It's interesting to note that 35% of those organizations with no security training are also the most concerned about their employees as a source of security incidents.

How much do your employees know about mobile security?

Training is not provided.



Training is provided.



The correlation between giving employees training and awareness of mobile security is hardly shocking. What is surprising, is the extent to which employees are seen as a risk and how few companies are using MDM solutions. This suggests that companies are relying on employees avoiding risk, instead of investing in the tools that can help enforce policies and prevent incidents. Even if companies were giving all staff thorough training on the changing threat landscape – and our research suggests that most aren't – this would not be an advisable approach.

76%

of respondents who said their company doesn't offer training also said their users know "little" about mobile threats. That's more than twice as many as those that do offer training (33%).

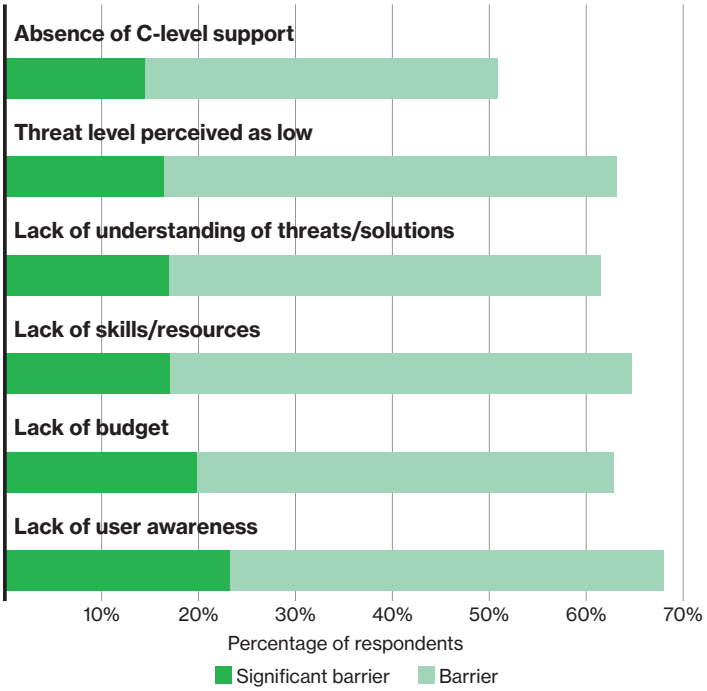
What's stopping them from doing more?

When asked about the barriers to mobile security, the most common reason given by respondents was the lack of user awareness about mobile security measures.

There isn't a single answer.

We asked respondents about six potential barriers to doing more about mobile security. Only one barrier – the absence of C-level support – was cited by less than 60% of respondents. When asked which barriers were significant, all six options scored between 14%–23%.

Why aren't companies doing more?



The situation is complex – on average, respondents said 2.6 of the barriers were significant in nature. There are two key lessons that we can learn from that.

Insecure coding strikes again.

As we were writing this paper, a major security incident hit the news headlines. A service used by many companies to send notifications – from "your cab is here" to "your payment has been made" – was found to be exposing security credentials. Initial reports indicate that it was bad coding on the behalf of the companies building the apps, not an inherent weakness in the service itself. This might seem relatively innocuous, but services like this are also used to send two-factor authentication codes – so an exploit could expose critical systems.

1. Budget is not the primary barrier.

Lack of budget was seen as a significant barrier by 20% of respondents. This may be a result of the broader challenges that IT departments face, rather than anything specifically related to mobile security.

61%

of respondents said they expect their mobile security budget will increase in the next 12 months. 38% expect it will stay the same.

We found that budgets have increased and are expected to increase. 52% of respondents said that their mobile device budgets have increased in the past 12 months – just 2% said that they had decreased.

- 61% expect their budgets to increase in the coming year while only 2% expect budgets to decrease.
- 82% of those who said their budget increased significantly last year say it is also doing so in the coming year.
- 86% of those who are increasing spend say that they see threats as increasing in the next year, compared to just 53% of those who don't plan to spend more.
- 46% said that they had both seen an increase in the past 12 months and expected to see a further increase in the next year.

2. Lack of user awareness is holding companies back.

23% of respondents said that lack of awareness among device users was a significant barrier to mobile security. And only 12% say their device users know a lot about mobile security.

There appears to be a connection between lack of skills as a barrier and plans to increase the security budget. 27% of respondents who said lack of skills is a significant barrier have increased their budgets, compared to only 5% who said it is not a barrier.

62%

of respondents said that lack of understanding of threats and solutions is a barrier to mobile security. 17% said that it is a significant barrier.

How you can improve your mobile security.

Our research shows that only 14% of respondents have four basic security measures in place: changing all default passwords, encrypting all sensitive data sent across public networks, restricting access on a need-to-know basis and regularly testing security measures.

Nearly all respondents (93%) said that organizations should take mobile security more seriously. With this in mind, we have compiled the following recommendations to help you elevate your organization's mobile security. We have also included IoT-specific recommendations on page 15.

83%

agreed that organizations are complacent about mobile security, and 24% of those strongly agreed.

	Baseline	Better	Best
Applications Reduce the risk of malicious and vulnerable applications.	Prevent employees from installing apps downloaded from the internet.	Deploy application management software/ endpoint security that controls which apps are installed, and scans those that are for vulnerabilities.	Create a custom app store and vet all apps that are added to it. Prevent users from installing apps from anywhere else.
Devices Improve device management, automating it as much as possible.	Deploy a device enrollment policy. This should include ensuring that all default passwords are changed. Create a formal BYOD policy detailing employee responsibilities. Implement a strong password policy and ensure adherence.	Implement a mobile device management (MDM) system. Enforce device encryption wherever possible.	Deploy mobile endpoint security/threat detection to all devices. Implement device segmentation, keeping personal and work data and applications separate.
People Increase user awareness and make sure you're prepared for an incident.	Provide regular security training including how to spot the early warning signs of an incident. Regularly review access to systems and data.	Test employee awareness of mobile security at least annually. And mandate additional training for anybody who doesn't get an acceptable score.	Train security ambassadors to act as champions for improved mobile security. Create an incident response plan that makes employees aware of what to do in the event of an incident.
Networks Reduce the use of less secure connections.	Create a policy on the use of public Wi-Fi. Encrypt all corporate-controlled Wi-Fi networks using WPA2 or later. Apply any updates to encryption software promptly. Educate users on the dangers of rogue and unsecured networks. Encourage them to verify the legitimacy of a network before connecting to it. Reconsider the use of 2G cellular data connections.	Deploy a VPN solution to any device that needs to access sensitive data over an unsecured network. Limit the use of Wi-Fi to approved networks. Create a private mobile network and limit access to all – or at least all sensitive – corporate resources for any mobile device not using it.	Change procurement policies to favor devices with 4G LTE over Wi-Fi. Deploy data loss prevention (DLP) software to limit data transfer, provide early warning and enable forensics.

Appendices

A: The Internet of Things.

Over a third (35%) of respondents who believe mobile security threats will increase in the next year said that new vulnerabilities from the Internet of Things (IoT) will be a contributing factor. Those using IoT were significantly more likely to say that downtime is a greater threat than data loss.

Nearly 60% of respondents said their organizations' mobile assets include IoT devices. This is quite high considering that most other estimates of adoption are below 30%.

This greater-than-expected use of IoT devices may be explained by the size of companies surveyed and the sectors they came from. Our sample is predominantly companies with over 250 employees with large numbers of mobile devices – and includes many from technology and manufacturing, both regarded as early adopters of IoT.

The good news is that this provides us with a sizeable sample of IoT users, helping us to better understand their security concerns and the precautions they are taking.

Almost four fifths (79%) of respondents said that IoT is the greatest security risk facing organizations. Many reports, including Verizon's State of the Market: Internet of Things 2017, have discussed the growing number of companies using IoT in core business processes, and how it has become mission-critical.

What challenges do IoT devices bring?

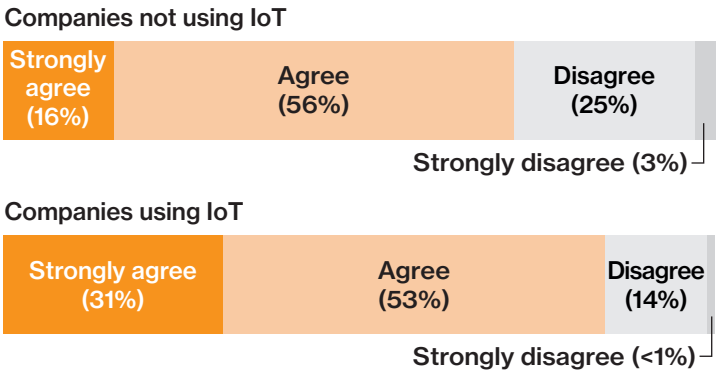
67% of respondents said that the security challenges of IoT devices are the same or mostly similar to those of other mobile devices. Yet, many IoT devices lack the fundamental security features that are typically part of smartphones and other devices.

Since most IoT sensors and devices are not owned by an individual in the same way as a smartphone or tablet, and many operate in remote locations, they can also be more susceptible to both physical tampering and network compromise.

26%

said that their current IoT security measures are very effective.

System downtime is a greater threat than data loss.



Respondents were asked which consequences of a security incident concerned them the most. 85% of organizations using IoT devices agreed with the statement that system downtime is a greater threat than data loss. 31% strongly agreed – that's nearly double those not using IoT (16%).

85%

of organizations using IoT agreed that system downtime is a greater threat than data loss, and 31% strongly agreed.

While worrying about disruption makes sense, it may also reflect a lack of understanding about some of the threats associated with using IoT devices. Considering the number of high-profile data breaches that exploited weaknesses in ancillary systems – such as heating, ventilation, and air conditioning (HVAC) – it's surprising that 12% of respondents aren't aware of the danger of IoT devices being used as a stepping stone to systems holding monetizable data. A further 39% are aware but unconcerned.

Awareness of stepping stone attacks.

Overall, most organizations felt that they are doing a fairly good job on IoT security. 81% said that they think their IoT security measures were quite or very effective. But when IoT is mission-critical and, in many cases, can provide an entry point to other systems and data, is "quite effective" good enough?

Secure your IoT devices.

By implementing the following six security practices, you can secure your IoT applications, protect sensitive data and avoid unnecessary downtime.

Encrypt data at rest and in transit.

Encryption is a powerful tool to protect data, but one that's not used as often as it should be. Only 47% of respondents said that they always encrypt data being transmitted over public networks.

For IoT applications handling sensitive data, such as medical and even personal location information, encryption is a must-have. We recommend using it for all applications. Many IoT devices don't store much information, but you should consider encrypting any data that your devices do hold – and always encrypt any authentication data.

Bake security in from the start.

With IoT projects, it's critical that security practices are built in from the start and not considered an afterthought. IoT is rapidly evolving, with many companies making bold moves and others racing to keep up. This can lead companies to rush to market, and perhaps compromise security as a result.

Device security systems help developers add security controls to endpoint devices. These systems have been tuned to the processing capacity of typical IoT devices. They can help with device hardening, including implementing firewall features that can block most network traffic to and from the device, only permitting explicitly-approved ports and IP addresses. Many also include security event alerting, providing vital early warning of attacks and enabling you to act quickly to reduce the impact.

Practice secure coding.

Only 42% of respondents said that they use secure development techniques. As well as code on the devices, many IoT applications rely on mobile apps and web-based portals. But many companies working on IoT projects, including hardware manufacturers, are new to building secure software.

It's not just your code that you have to worry about. Several commonly used libraries – including OpenSSL and gSOAP – have been found to have significant vulnerabilities[3,4] It's critical that organizations employ secure coding techniques and follow our next recommendation.

58%

of respondents said they don't practice secure coding techniques.

Enforce strong authentication and access control.

Only 39% of respondents using IoT said that they change all default passwords.

As the volume of devices increases, it's vital that organizations use rigorous authentication and access policies and put robust procedures in place to enforce them

Security credentialing is an effective way to enable strong authentication between devices and servers, and device-to-device. It can also protect data exchanged between any devices that leverage standard digital certificate protocols – which includes all leading smartphones, tablets and other devices.

Test, test and test again.

In the rush to get products to market, or show that IoT projects are delivering a return on investment, there can be pressure to cut testing time. This is a false economy and can lead to vulnerabilities being missed and making it into live systems. Thorough and ongoing penetration testing is critical to achieving and maintaining adequate levels of protection.

Plan for updates.

It's critical that you can perform updates securely "over the air" (OTA). As well as enabling you to improve functionality for users, OTA updates mean that you can patch any vulnerabilities and take advantage of new security practices as they emerge.

B: Every industry is affected.

Compared to other industries, retail and hospitality are disproportionately concerned about payment card data and healthcare organizations about medical data. Beyond these, there are relatively few differences between industries when comparing concerns about securing data.

Healthcare companies are most likely to have suffered data loss or downtime as a result of an incident involving a mobile device – 35% had in the past year. The average across all industries is 27%. Cybercriminals consider all industries as targets.

The percentage of companies that said mobile devices are a risk varied from 79% in manufacturing to 90% in professional services. For those that said mobile devices are a significant risk, the range was from 16% in government to 39% in professional services.

Across all industries, a majority of respondents said that disruption of systems is a greater threat than the loss of data – from 73% in manufacturing to 85% in financial services.

Financial services

25%

experienced a mobile-related incident; 18% a major one with lasting repercussions.

85%

said mobile devices are a risk; 37% said they're a significant one.

Banking employees have access to customer data in their normal work day that would be a cybercriminal's dream; and it's not just data that's easy to monetize. Investment banks and other non-commercial entities have access to all kinds of sensitive information. Espionage is a very real risk when employees have access to sensitive data. That's why it's particularly concerning that 39% of financial services companies fail to regularly check security systems and processes.

Financial services companies were most likely to agree that IoT is the greatest security threat facing organizations – 93% agreed, with 19% of those strongly agreeing. Driven by new entrants, the fintech revolution is now forcing even incumbent players to innovate and adopt new technologies – mainly using IoT technologies – more quickly.

Government

33%

experienced a mobile-related incident; 11% a major one with lasting repercussions.

85%

said mobile devices are a risk; 16% said they're a significant one.

Public sector organizations – including state, national and federal government – are entrusted with vast amounts of highly sensitive information. And the costs of a data breach can go well beyond financial.

While security is obviously a top concern, complex departmental hierarchies and disparate or outdated IT infrastructure can make it difficult to enforce consistent policies. That's perhaps why government organizations were the second most likely to say that they themselves have suffered downtime or data loss (33%).

But they certainly recognize the risks of mobile devices, and are taking employee training seriously. They were most likely to say that they thought mobile devices pose a risk (85%); and that they give employees training about the risks on an ongoing basis (57% versus 35% across all industries).

Healthcare

35%

experienced a mobile-related incident; 22% a major one with lasting repercussions.

87%

said mobile devices are a risk; 29% said they're a significant one.

Healthcare has the unenviable task of guarding large amounts of highly sensitive and personal data, while also providing quick access for medical practitioners. These risks need to be weighed against speed and accessibility. Complicated or unwieldy access systems could do more harm than good, especially in emergency situations. Perhaps that's why healthcare companies were most likely to say that they have knowingly sacrificed security for expediency or business performance – 41% compared to an average of 32% across all industries.

That might be an understandable sacrifice; but it's having consequences. Healthcare companies were the most likely to say that they had suffered a breach in the past year – over a third (35%) had. This is concerning when you consider the highly confidential nature of medical data. And when IoT is involved there are even greater risks to consider; imagine if a threat actor gained control of medical equipment or devices.

Manufacturing

19% experienced a mobile-related incident; 10% a major one with lasting repercussions.

79% said mobile devices are a risk; 21% said they're a significant one.

There are always people striving to make the same things more cheaply. One way of achieving this is by letting someone else do all the research and development and then stealing their intellectual property (IP). Employees could have access to all kinds of IP – algorithms, recipes, machinery details, plans or cutting-edge creative concepts – through their mobile devices.

The 2017 DBIR found that cyberespionage was the predominant motivation for breaches in this sector. But manufacturers also face risks from operational downtime as a result of breaches. A halt or delay to operations – even of a few hours – can be extremely costly in a production environment.

While the number of manufacturing companies that had experienced an incident was low compared to other sectors, it was still nearly one in five (19%). And over three quarters (79%) agreed that mobile devices pose a risk.

Professional services

29% experienced a mobile-related incident; 18% a major one with lasting repercussions.

90% said mobile devices are a risk; 39% said they're a significant one.

Professional services organizations are entrusted with the protection of highly sensitive information, including clients' personal information, lawsuits, tax information and intellectual property. They are also likely to process payment card details. This puts them at risk of financially motivated attacks, as well as personally motivated attacks, hacktivism and espionage.

These organizations are ramping up their use of mobile devices and IoT technology. Professional services companies were most likely to say that they thought that the risks associated with mobile devices have increased significantly in the past year, with 35% agreeing with that statement. And 71% said that they expect the threats to grow in the coming year.

Retail and hospitality

16% experienced a mobile-related incident; 15% a major one with lasting repercussions.

82% said mobile devices are a risk; 22% said they're a significant one.

Organizations in the retail and hospitality sectors are a prime target for financially motivated cyberattacks as they are entrusted with vast amounts of payment card data. Retailers were significantly more concerned about their customers' financial data being compromised (67%) compared with other industries (46%).

Retail and hospitality companies face distinctive challenges when it comes to mobile security. Many of them have large numbers of employees, often employed on part-time or seasonal contracts. These employees may not take security precautions as seriously as full-time or permanent employees.

It's not surprising then that companies in these sectors were the most likely to say that employees are their biggest concern, with 29% putting them at the top of their list of potential breach sources.

Technology

31% experienced a mobile-related incident; 23% a major one with lasting repercussions.

88% said mobile devices are a risk; 27% said they're a significant one.

Of all sectors, you might expect technology to be the most savvy when it comes to mobile security. But it may also face greater risks. Technology companies have experienced more major incidents (23%) than those in any other sector. Perhaps this is because they're more inclined to adopt the latest devices and IoT technology – which despite its potential, may also make them a target for cyberattacks.

They certainly recognize the inherent dangers, with 88% saying mobile devices are a risk. And they're taking precautions. Respondents classifying their employer as a technology company were most likely to say they expect their security budget to grow significantly in the next year (18%). They also said they are devoting the largest share of their security budget to complying with regulation – 51% compared to an average of 43% across all industries.

C: Public Wi-Fi presents a real threat.

With more and more people wanting to be online all the time, it's easy to understand the appeal of free public Wi-Fi. 71% of our respondents said that they use it for work tasks—many even when they know that it's officially prohibited. As we've reported, lack of user awareness is a leading barrier to better mobile security. Do your users understand the dangers of using public Wi-Fi?

Are you being watched?

Unsecured connections, commonly found in hotels and on trains, are a particular risk. Anyone on the same network could eavesdrop on your online activities without you knowing it. Yes, that guy a few tables away could be looking at every page you load and every form you submit. It's even possible for him to read your emails. And it's easier than you might think.

Are they who they say they are?

You wouldn't connect to a network called "Get hacked here," but how many people automatically trust that "Hotel free Wi-Fi" is legitimate and safe? It might be nothing to do with where you're staying. Hackers create fake access points with safe-sounding names like this and wait for gullible users to connect. They can also spoof genuine Wi-Fi networks and intercept transmissions in what's known as a "man-in-the-middle" attack. Either way, they get access to your private communications.

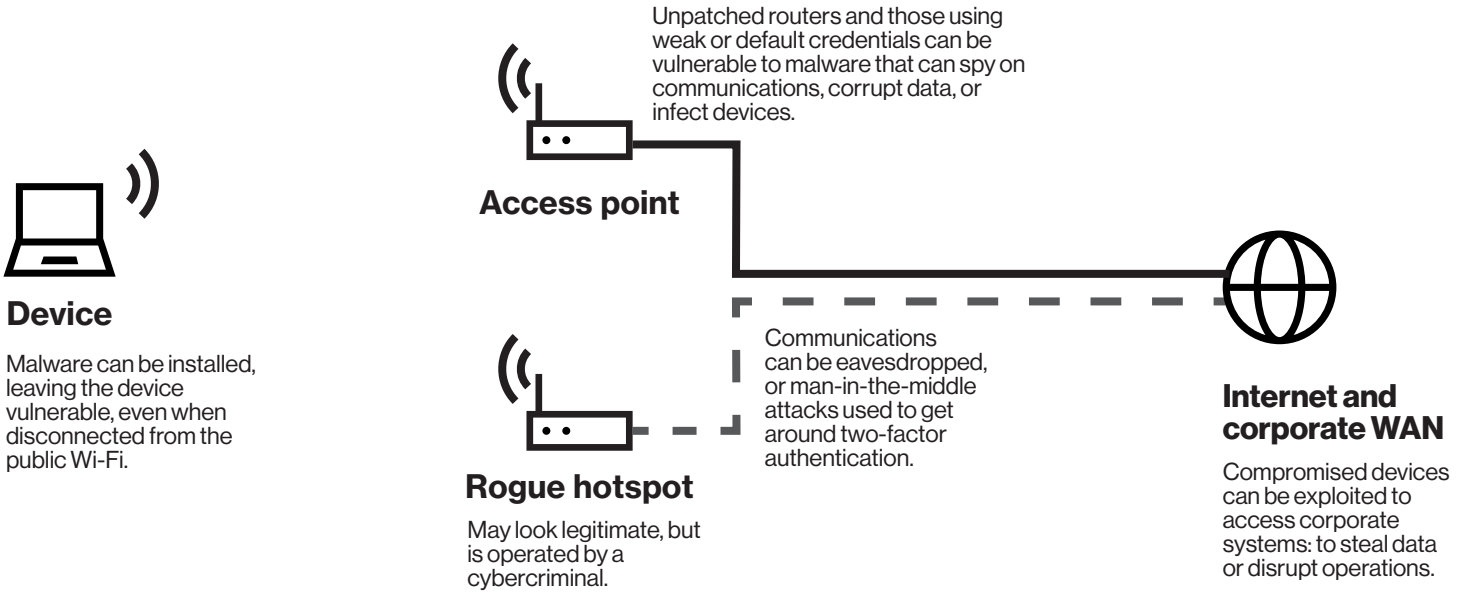
Can you trust the connection?

Even secured Wi-Fi has its dangers. The owner might not be using even the most basic security precautions, like strong authentication. If they're using default credentials on a router, it's even easier for hackers to get in. And if the router is compromised, your data is at risk while in transit and your device could be infected.

Even if you don't access confidential data or sensitive systems while on Wi-Fi, you might give away other personal details and credentials that hackers could use later on.

Malware can stay on your device long after you disconnect from a network. It could remain in action, gathering data and credentials to send to the hacker. Worse still, that malware could go on to infect other devices on your network, including servers hosting mission-critical applications.

Public Wi-Fi presents many dangers.



D: 4G LTE can help improve security.

LTE is wireless technology based on specifications developed by 3GPP, an international standards organization. It offers high bandwidth, low latency and advanced security. It's now widely available around the world, from Afghanistan to Zimbabwe.

Secure storage.

With 4G LTE, a Universal Integrated Circuit Card (UICC) token holds credentials and secure data for accessing services provided by the mobile network. The private key is created when the UICC is manufactured, and is only shared with the carrier in a secure way, preventing this data from being intercepted and used for illegitimate purposes. Personal Identification Number (PIN) and PIN Unblocking Key (PUK) mechanisms are enforced on the UICC to secure access to data or applications on the LTE network. This provides cryptographic primitives and secure storage of key material that cannot be corrupted by the surrounding hardware and software on the handset. The UICC itself is a tamper-resistant compute platform and supports multiple cryptographic algorithms.

Airlink encryption.

When 2G was the prevailing standard, it was possible to intercept mobile phone calls as they passed over the radio waves. From 3G onwards, encryption of data transmissions has made this much more difficult. LTE encrypts both data and signaling to prevent it being overheard on the radio access interface. Most LTE networks support 128-bit encryption.

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 any kind of man-in-the-middle attack. The UICC contains the necessary authentication algorithms and certificates, which aids in the secure accessing of the network. During initial attachment to the network, a temporary mobile subscriber identity (TMSI) is used instead of the international mobile subscriber identity (IMSI) to protect the subscriber from being identified.

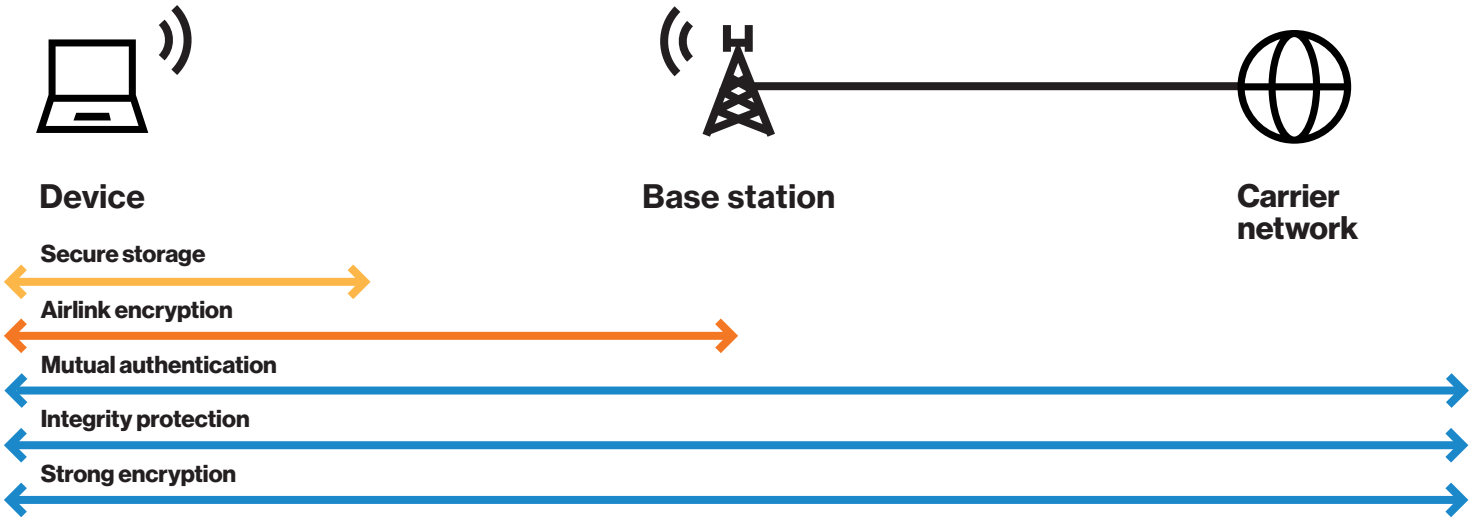
Integrity protection.

Signaling is the means by which the network and the user's handset exchange messages to verify identity and control calls. This has been exploited in earlier mobile standards to spoof identity and intercept calls and data. Integrity protection is used to verify that the signaling has not been modified over the radio access interface 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.

Stronger encryption.

The use of 128-bit keys doubles the key strength compared to previous standards. With 64-bit keys there are 1.85×10^{19} possible permutations; with 128, that goes up to 3.40×10^{38}. This means that a vastly greater level of effort is required to break the encryption.

LTE enhancements improve end-to-end security.



E: About this research.

In the second half of 2017, Verizon commissioned an independent research company to survey over 600 professionals involved in procuring and managing mobile devices for their organizations.

The respondents cover a wide range of industries: financial services, government, healthcare, manufacturing, professional services, retail and hospitality, and technology.

And they represent a range of business sizes – from 250 employees up. 16% worked for organizations with under 500 employees, and 22% for organizations with 10,000 or more.

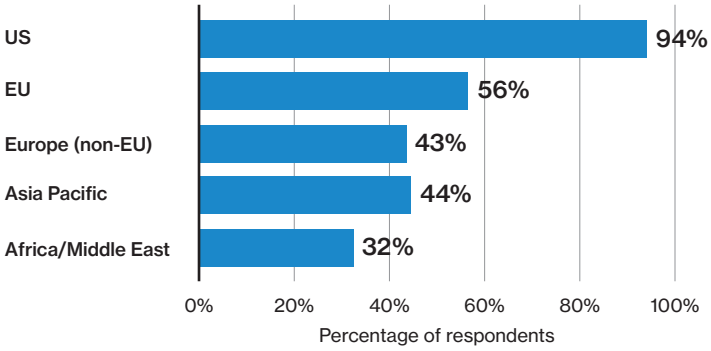
Half (50%) of the organizations studied have 1,000 or more mobile devices in use – more than a fifth (22%) have 5,000 or more.

42% of participants have a role in IT/telecoms, the rest cover a wide range of functions including senior leadership (19%). 64% said that they influence provider selection, 42% control budgets and 27% are specifically responsible for device security.

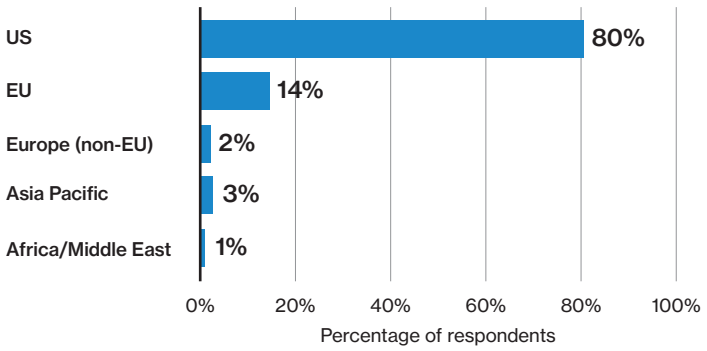
83% of those taking part are based in the US, the remaining 17% from the UK. These quotas enabled us to understand the differences between organizations in North America and Europe. As it turns out, the differences were minor, partly because most respondents have a global perspective.

Over 90% said that they do business in the US, over 50% in the EU, over 40% in non-EU Europe and Asia Pacific, and over 30% in the Middle East and Africa.

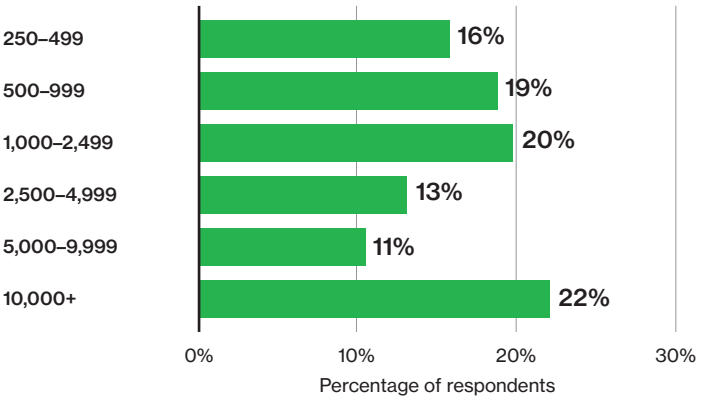
Where respondents do business.



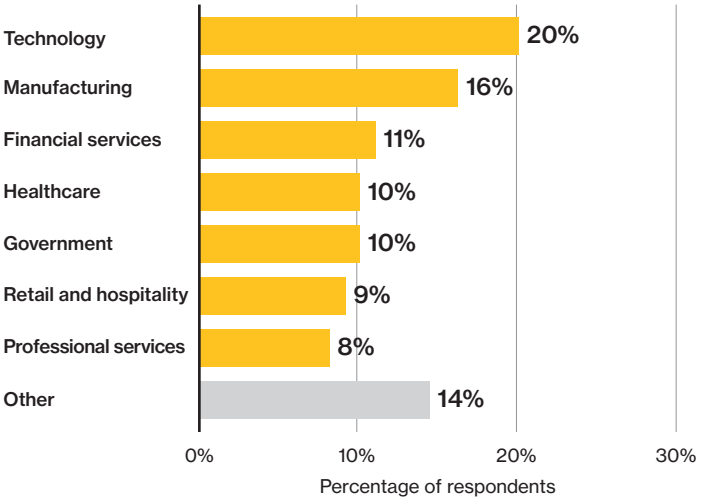
Where respondents do most business.



By number of employees.



By industry.



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.

As one of the largest network providers, we draw on the experience of our cybersecurity experts and help to protect valuable information for organizations of all sizes. Our global Network Operations Centers and Security Operations Centers process more than one million security events every day, so we understand the rapidly changing nature of cyber threats.

We're the only provider recognized by industry analyst firm Gartner as a leader in both Network Services and Managed Security Services in its 2017 Gartner Magic Quadrant reports.

We're also leading by example. Our business operates under a rigorous information security policy, and we maintain physical, electronic, and procedural safeguards of all our internal systems. Policy and governance is the cornerstone of any good security program, so we've created enterprise-wide policies that conform to the ISO 27002.2005 and NIST standards for the protection of customer information. We have operational standards that reflect these corporate policies, and an adherence program.

Verizon secures your information by:

- Employing strong user authentication technology, so that only authorized users and devices can connect to our wireless network and systems.
- Implementing internal and external security procedures to guard our networks and applications against unauthorized access.
- Installing firewalls and intrusion detection sensors to notify IT staff in the event of an attack on the network.
- Monitoring our wireless networks around the clock at our Network Operations Centers.
- Maintaining an active security patch management process to deploy updated software releases when security vulnerabilities appear.

Finding a partner to trust with your network security isn't easy—but it is critical. 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.

Data Breach Investigations Report

The cybersecurity answers you want, straight from the experts. The 2017 Data Breach Investigations Report (DBIR) is our foremost publication on security and one of the industry's most respected sources.

Download the report ›

State of the Market: IoT

IoT has always looked like a game-changer. Now, the tools are in place to overcome concerns around security, interoperability and cost. Find out why 2017 is the year IoT will become central to organizational decision making.

Download the report ›

Payment Security Report

Almost half of all organizations fail to maintain PCI DSS compliance. Read the 2017 Payment Security Report to discover which controls they didn't have in place, and how you can avoid the same fate.

Download the report ›

Data Breach Digest

Read the Data Breach Digest for the story of Verizon's most intriguing cybercrime investigations. Learn about the attacker's tactics, the victim's mistakes and the scramble to limit the damage.

Download the report ›

We offer best-in-class products to secure mobile devices, content, and applications. With Verizon, you can choose the most effective security solution for your business needs. **verizonenterprise.com/Support/sales/**

1. Pages.nist.gov/800-63-3/sp800-63b.html
2. kensington.com/a/312684
3. nvd.nist.gov/vuln/detail/CVE-2014-0160
4. nvd.nist.gov/vuln/detail/CVE-2017-9765

verizonenterprise.com