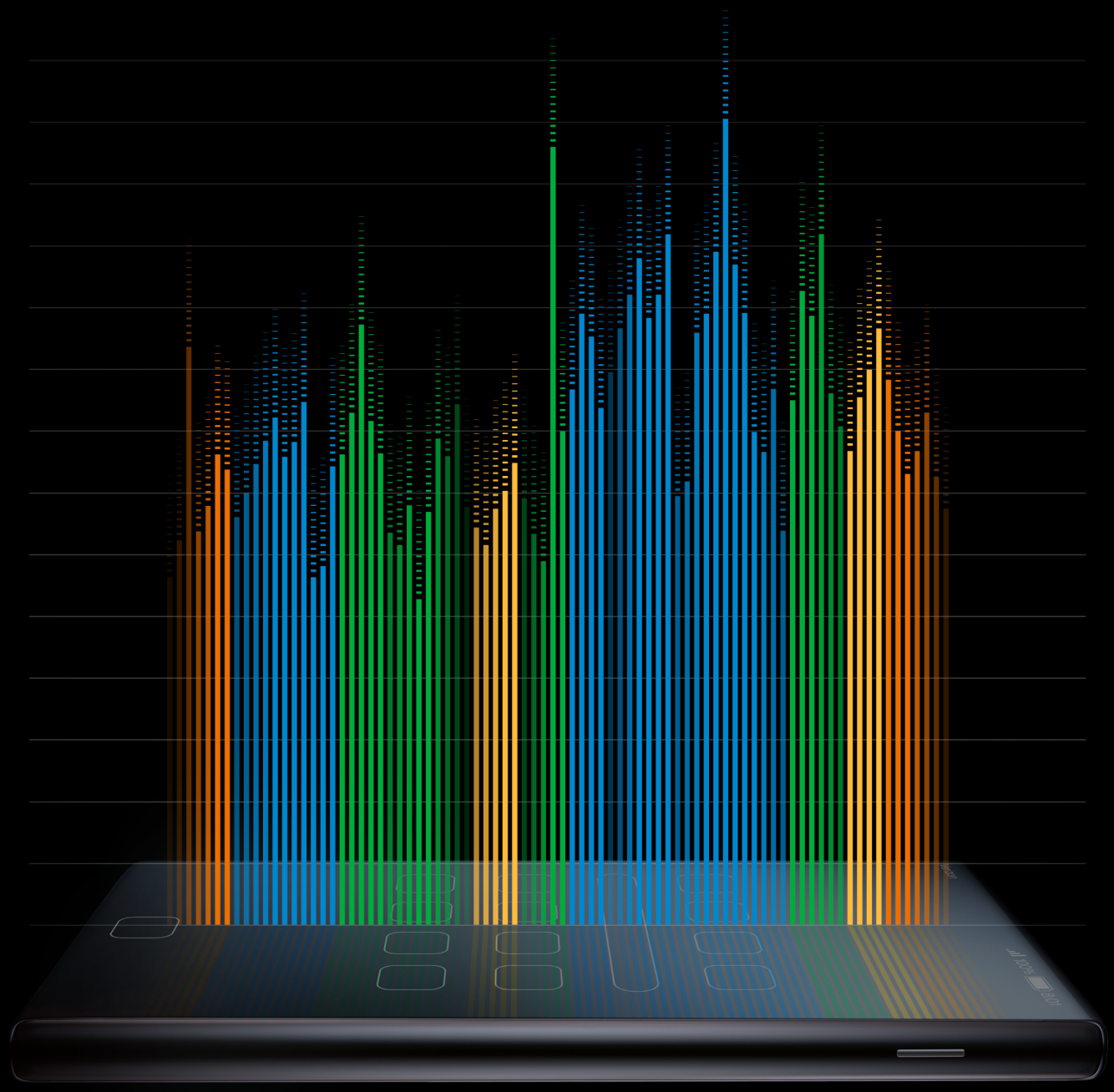
Mobile Security Index 2021



verizon

About this report

To help you assess your mobile security environment and calibrate your defenses, we've produced this fourth annual Verizon Mobile Security Index. To create it, we worked with Asavie, Check Point, BlackBerry Cylance, IBM, Lookout, MobileIron, NetMotion, Netskope, Proofpoint, Qualcomm, Thales, VMware and Wandera—all leaders in mobile device security. They provided additional information, including incident and usage data. We also commissioned an independent survey of 856 professionals responsible for the buying, managing and security of mobile and Internet of Things (IoT) devices.

The Federal Bureau of Investigation (FBI), Europol and the U.S. Secret Service also provided valuable input. We'd like to thank all our contributors for helping us to present a more complete picture of the threats that affect mobile devices and what is being done to mitigate them.

For more information on our survey, see page 86.

Table of contents

00

Foreword 04
Mobile Security Index cheatsheet 06

01

The state of mobile security 08
Compromises may be down, but the threats are growing. 09

02

Let's start just calling it "work." 13
Out of office 14
Working personas 18
Bring your own. 20
Securing BYOD/BYOPC programs 22
Small, but mighty 24
5G and multi-access edge computing 26

03

The threats are real. 28
The number compromised was down. 29
What do companies sacrifice security for? 33
Shadow IT 34

04

The mobile threat landscape 35
04.1 People and behaviors 37
VAPs not VIPs 38
Phishing 38
The Covid-19 effect 41
QRiosity can be dangerous. 42
Attack case study: Clorox 43
Business email compromise 44
Securing against phishing 45
Credential theft 48
Inappropriate use 49
Acceptable use and remote workers 51
04.2 Apps 52
Trends in app use 53
App permissions 54
Password snooping 56
Leaky apps 57
Malware 58
Ransomware 59
Attack case study: Lucy ransomware 60
Securing against malware 61
04.3 Devices and things 62
Out-of-date operating systems 63
Lost or stolen devices 65
IoT devices 67
Securing IoT devices 68
04.4 Networks and cloud 69
Risky networks 70
Cloud 74
Securing against network threats 76

05

Looking ahead 78
Drivers of change 79
The future 81
Conclusion 83

06

About this report 84
Terminology 85
Survey methodology 86

07

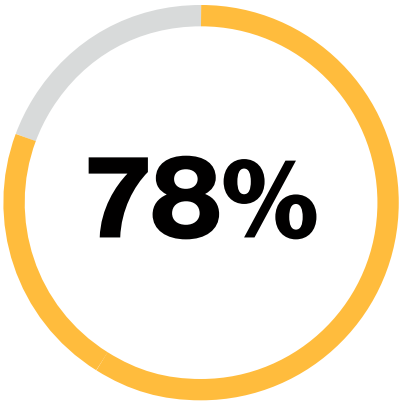
Contributors 87
Security companies 88
Law enforcement 93

08

Further reading 94
Verizon thought leadership 95
Additional resources from government and law enforcement agencies 97

Foreword

Cybersecurity is not a new issue, but the stakes are getting higher. The scale of regulatory penalties is growing, and customers—consumers, businesses and public-sector organizations alike—are becoming more sensitive to the issue. In the past, many consumers saw little difference between the security postures of the companies—such as banks and retailers—pursuing their business, and so it didn't sway their loyalty. That's changing, and consequently lots of companies are responding by making security and data privacy central to their value proposition.



More than three-quarters of companies think that data privacy will be a key brand differentiator in the future.

For more than a decade, Verizon has published some of the preeminent reports on cybersecurity, including the Data Breach Investigations Report (DBIR). This is the fourth edition of the Mobile Security Index. As the name suggests, it focuses on the threats to mobile devices; what defenses companies have in place to thwart these attacks; and how often those fail, leading to a mobile-related compromise.

One of the key themes of the 2020 Mobile Security Index was mal-innovation. We talked about how cybercriminals were constantly finding new and often imaginative ways to carry out attacks. In another life, where their motives weren't nefarious and the outcomes not so damaging to so many, the creativity and ingenuity shown by some of the attackers would merit fame and accolades.

Sadly, mal-innovation continues apace, and we saw many new examples in 2020. COVID-19—you didn't think that we'd not mention it, did you?—provided cybercriminals with new opportunities. Criminals were able to craft tailored phishing attacks very quickly. But that's no longer a surprise. It doesn't take a pandemic for phishing gangs to identify new ways to exploit human weaknesses to further their attacks.

Another of the key themes of our 2020 report was how mobile devices are not just being used more, but used for more. In large part driven by apps and data in the cloud, mobile devices have evolved from being a handy companion into an essential business tool. Today, you can buy a watch that has much of the functionality smartphones had just a couple of years ago. Smartphones, tablets and other mobile devices can now be used to access core systems, edit spreadsheets and perform other mission-critical tasks.

When we asked respondents to our latest survey to rate how crucial mobile is to their business on a 10-point scale, 71% answered 8 or higher. But with the increased reliance on mobile devices, the risk has grown too. Mobile devices are subject to all the same risks as non-mobile user devices, plus some of their own:

Amplified risks

Mobile devices can be subject to attacks that could happen on any device, but sometimes the mobile device makes them more likely to be successful.

An example is a phishing attack. Several of the ways users spot a malicious email or website are less obvious on a small screen, meaning users may be more likely to fall for an attack.

Specific risks

Mobile devices are significantly more prone to loss and theft. This can lead to the exposure of data, but often the biggest impact is on productivity.

Because they are often used in public places—like trains and coffee shops—mobile devices are susceptible to eavesdropping, both physical and electronic.

Gateway risks

Attackers can exploit mobile devices to acquire data from the cloud and other systems that they connect to.

They can also be attacked to capture credentials, which can then be used to gain access to data in other systems.

We couldn't really write this report without discussing the impact the COVID-19 pandemic has had on the nature of how we work. The number of remote workers has been growing for years, but in many companies—including Verizon—working from home went from being the exception to being the rule virtually overnight. Unsurprisingly, this led some to cut corners, including on security. Nearly a quarter (24%) of respondents to our survey said that their organization had sacrificed the security of mobile devices to facilitate their response to restrictions put in place due to the pandemic.

Read on to learn more about the mobile security environment and understand its risks. We hope that this insight will help you to strengthen your mobile security as your digital transformation journey—and evolution to the new world of work—unfolds.

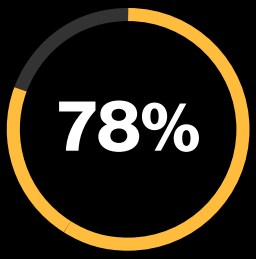
The findings of this report are based on a survey of 856 professionals responsible for the procurement, management or security of mobile devices. Unless stated otherwise, quoted statistics are from this survey. Other findings are based on data supplied by our contributors: Asavie, Check Point, BlackBerry Cylance, IBM, Lookout, MobileIron, NetMotion, Netskope, Proofpoint, Qualcomm, Thales, VMware and Wandera.
For full details of the methodology, please see page 86.

Mobile Security Index cheatsheet

The threats are rising.

Two-fifths of respondents said that they think that mobile devices are the company's biggest IT security threat. Of the rest, 85% said that mobile devices are at least as vulnerable as other IT systems.

Forty percent said that mobile devices are the company's biggest security risk.



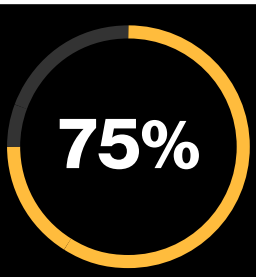
Seventy-eight percent expected home working to remain higher even when COVID-19 is no longer an issue.

Driven by increased home working

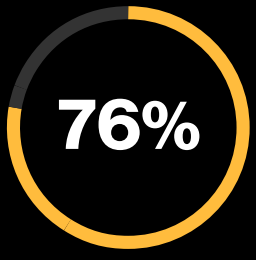
A large majority (79%) had seen remote working increase as a result of COVID-19. Most (70%) expected remote working to fall again, but over three-quarters said that it would remain higher than before lockdown.

And expanded use of cloud

Respondents said that nearly half (46%) of their IT workloads were run in the cloud. Three-quarters said their reliance on cloud-based apps is growing.



Seventy-five percent said that their business's reliance on cloud-based apps is growing.



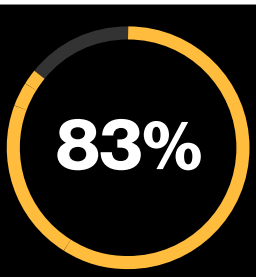
Seventy-six percent said that they'd come under pressure to sacrifice the security of mobile devices for expediency.

Putting pressure on IT

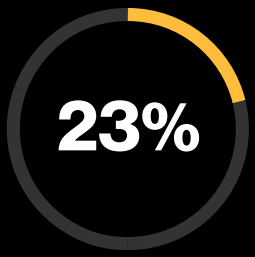
Growing threats and never-ending pressure from the organization are putting IT in a difficult position. Over three-quarters had come under pressure to sacrifice mobile device security to help meet deadlines and other business goals. And 75% of those succumbed.

And increasing concerns

The vast majority (82%) of respondents that expressed an opinion said that within five years their company will rely on networks it doesn't own, like home broadband and cellular, more than ones it does. More than half (58%) said they struggle to reconcile differing mobile demands from across the business.



Eighty-three percent said that they are concerned about the growth of "shadow IT."[1]



Twenty-three percent were aware that their company had experienced a mobile device-related security compromise.[2]

Reported compromises are down.

Fewer respondents in our latest survey were aware of their company having suffered a mobile-related security compromise.

But the severity remains high.

Over half of those that had suffered a compromise said that the consequences were major. Just 12%, less than one in eight, said that the consequences were minor.

Fifty-three percent said that the consequences of a breach they suffered were major.

1 Users or departments making their own IT decisions and purchasing without oversight.
2 All 856 respondents.

The state of mobile security

01

Each edition of this report has seen the number of companies suffering mobile security compromises rise. Until now. While this is good news, there are many reasons to believe that the picture isn't as rosy as this finding might suggest. More than one in five surveyed companies had experienced a compromise involving a mobile device in the preceding 12 months. And further, the severity of the consequences remained high.

Compromises may be down, but the threats are growing.

Fewer companies were aware of successful mobile-related attacks.

This is the fourth year that Verizon has published this report. And this time the percentage of companies that admitted to having suffered a mobile-related security compromise is the lowest we've seen—just 23%.[3] But hold the Champagne. Nearly one in four companies suffering a mobile device attack is not cause for celebration.

By way of comparison, a recent report by Thales noted that 26% of global respondents had experienced a data breach of any kind in the previous 12 months.[5]

One factor affecting these results is that the pressure on companies to sacrifice security was higher due to the measures needed to cope with COVID-19. This is highly likely to have inflated the sacrifice figures.

Companies were also likely to have been distracted. This could mean that they haven't spotted compromises, or if they did spot them, they have not thoroughly traced them back to identify all involved sources.

It's also likely that cybercriminals were still modifying their methods when we did our survey. While attacks like phishing could continue as normal—and, in fact, COVID-19 gave hackers new opportunities—these attacks are less likely to be traced back to a device type.

The share of companies sacrificing security went up, but fewer suffered a compromise.

Report	Sacrificed security	Experienced compromise	Multiplier*
2018	32%	27%	2.4x
2019	48% ▲	33% ▲	1.9x
2020	43% ▼	39% ▲	2.0x
2021[4]	**45% ▲**	**23% ▼**	**1.5x**

Figure 1. Has your organization experienced a security compromise involving mobile/IoT devices during the past year? Has your organization ever sacrificed the security of mobile devices (including IoT devices) to "get the job done" (e.g., meet a deadline or productivity targets)? [n=601, 671, 876, 856]

*Increased likelihood that an organization that sacrificed security suffered a mobile-related security compromise. For example: Companies that sacrificed security in 2021 were 1.5 times as likely to suffer a mobile-related security compromise.

3 All 856 respondents.
4 Ibid.
5 Thales Data, Threat Report Global Edition, 2020. Based on research carried out by IDC in November 2019.

The risks remain high.

Companies see themselves as at risk.

Despite the drop in known compromises, more than one in five companies experienced the loss of data or significant disruption to operations, or both. Just 14% of respondents thought that there was little or no risk associated with mobile devices.

More than two-thirds of respondents said that the risks associated with mobile devices had increased in the past year. And half (50%) said that mobile device risks are growing faster than others.

Few thought that there was no risk associated with mobile devices.

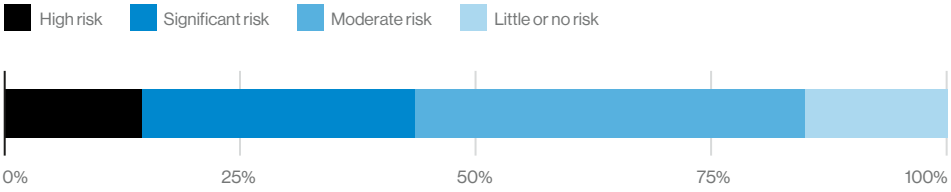


Figure 2. How would you assess your organization's risk from mobile device threats? Consider any security risk stemming from the use of smartphones, tablets or laptops using mobile data. [n=590]

Most thought that the risk associated with mobile devices grew in the past year.

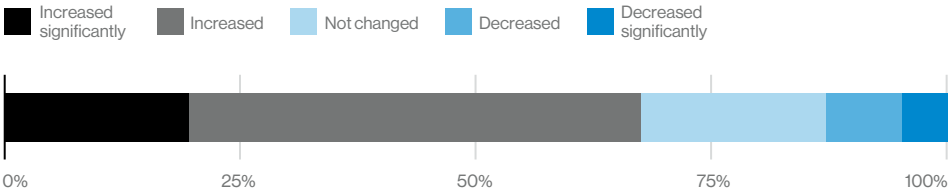


Figure 3. How do you think the security risks associated with mobile devices have changed in the past year? [n=591]

Half thought that mobile device risks were growing faster than others.

Figure 4. Which of the following statements regarding the security of mobile devices do you agree with? Mobile device threats are growing more quickly than other threats. [n=598]

Companies are still failing on the basics.

Since the first edition of this report, back in 2018, we have tracked how many companies have had four basic protections in place. These precautions were chosen based on some of the recurring problems identified in our sister publication, the Verizon Payment Security Report.

Over the years, the share of companies in compliance with these protections hasn't changed much. Until now. In previous reports, the share of companies in compliance with all four hovered around 12%, give or take 1 percentage point (pp). In our latest review, just 9% had all of them in place.

Despite not even having some of the most basic precautions in place, most respondents thought that any security or misuse issues would be spotted quickly. This mirrors our findings in previous years.

The four basic protections

Which of the following statements match your organization's security policies?

1. We change all default/vendor-supplied passwords
2. We always encrypt sensitive data when sent across open, public networks
3. We restrict access to data on a "need-to-know" basis
4. We regularly test our security systems and processes

Find out more.

Learn more about compliance with the Payment Card Industry Data Security Standard (PCI DSS) in the Verizon 2020 Payment Security Report (the ninth edition).

verizon.com/paymentsecurityreport

Companies with all four basic protections in place

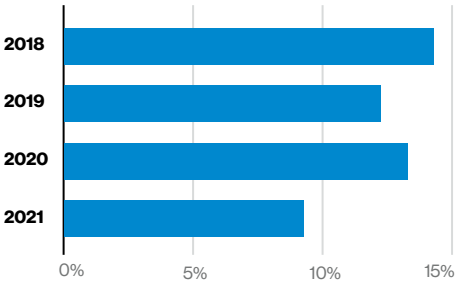


Figure 5. Which of the following statements match your organization's security policies? [n=601, 671, 856, 598]

Few had four basic security measures in place.

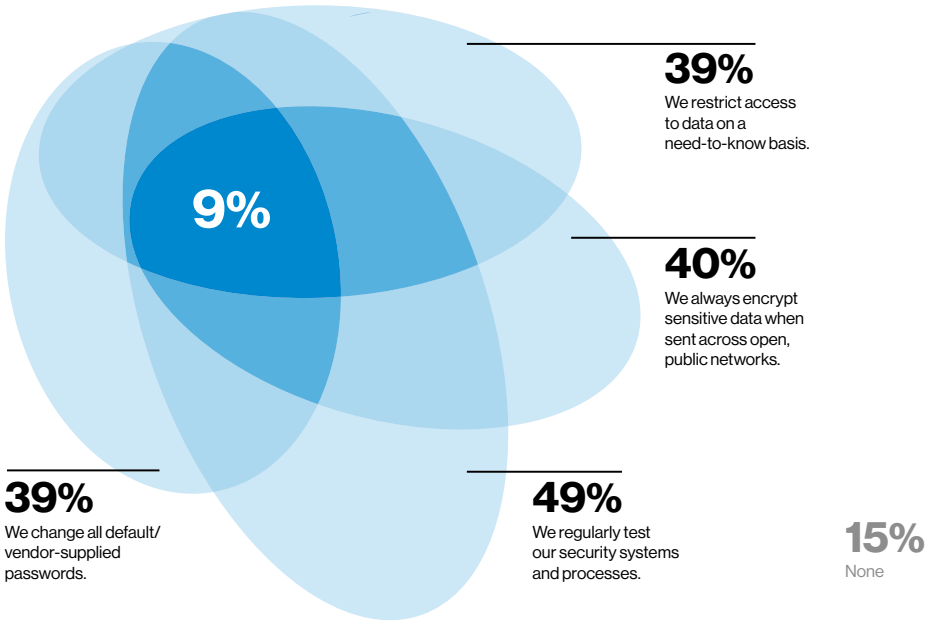


Figure 6. Which of the following statements match your organization's security policies? [n=598]

Companies remain confident in their defenses.

Despite the risks and numerous indications throughout our survey that companies have insufficient defenses in place—both in terms of security solutions and processes—companies were confident that they would spot compromises and misuse quickly.

This isn't new; we've seen similar confidence in our previous surveys. Nor is the fact that despite this, companies realize that they have more to do. In our latest survey, 81% of respondents agreed that organizations need to take the security of mobile devices more seriously.

Most thought they'd spot a compromised device quickly.

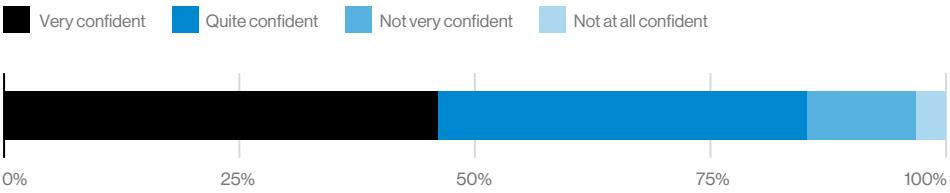


Figure 7. If a mobile device was compromised, would you spot it quickly? [n=591]

Most thought that the risk associated with mobile devices grew in the past year.

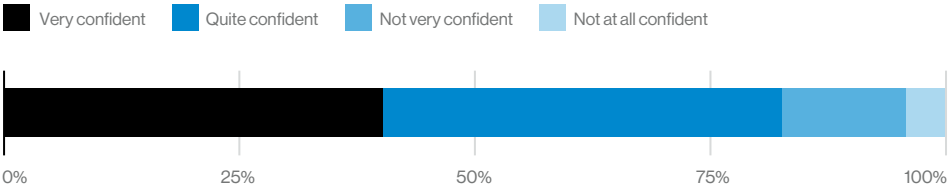


Figure 8. If one of your employees misused a company device, would you spot it quickly? [n=592]

Let’s start just calling it “work.”

02

In the past, working from home was thought of as a special case. That attitude had been changing, slowly. Then COVID-19 hit and companies were forced to reevaluate virtually overnight. The shift may not have been through choice, but now even some leaders with the most entrenched objections to home working have changed their minds. It seems that necessity is also the mother of evolution. The “new normal” remains uncertain, but it’s a safe bet that more flexible working arrangements are going to be part of it.

Out of office

You don't need a research report to tell you that there was a massive increase in the number of people working from home in 2020. Remote working has become commonplace and things are unlikely to ever go back to the way they were. Numerous companies have announced long-term—or even permanent—work-from-home policies and plans to reduce their property footprint.

Netskope has called this phenomenon "inversion." Its research found that the ratio of remote workers to others went from one in four at the start of 2020 to two out of three by the summer. And that pattern continued throughout the rest of the year.

> **"We anticipate never going back to five days a week in the office, that seems very old-fashioned now."**
>
> —Alan Jope, Unilever CEO[6]

Almost two-thirds (66%) of respondents said that they expect the term "remote working" will have disappeared within five years.

The ratio of remote workers to others has "inverted."

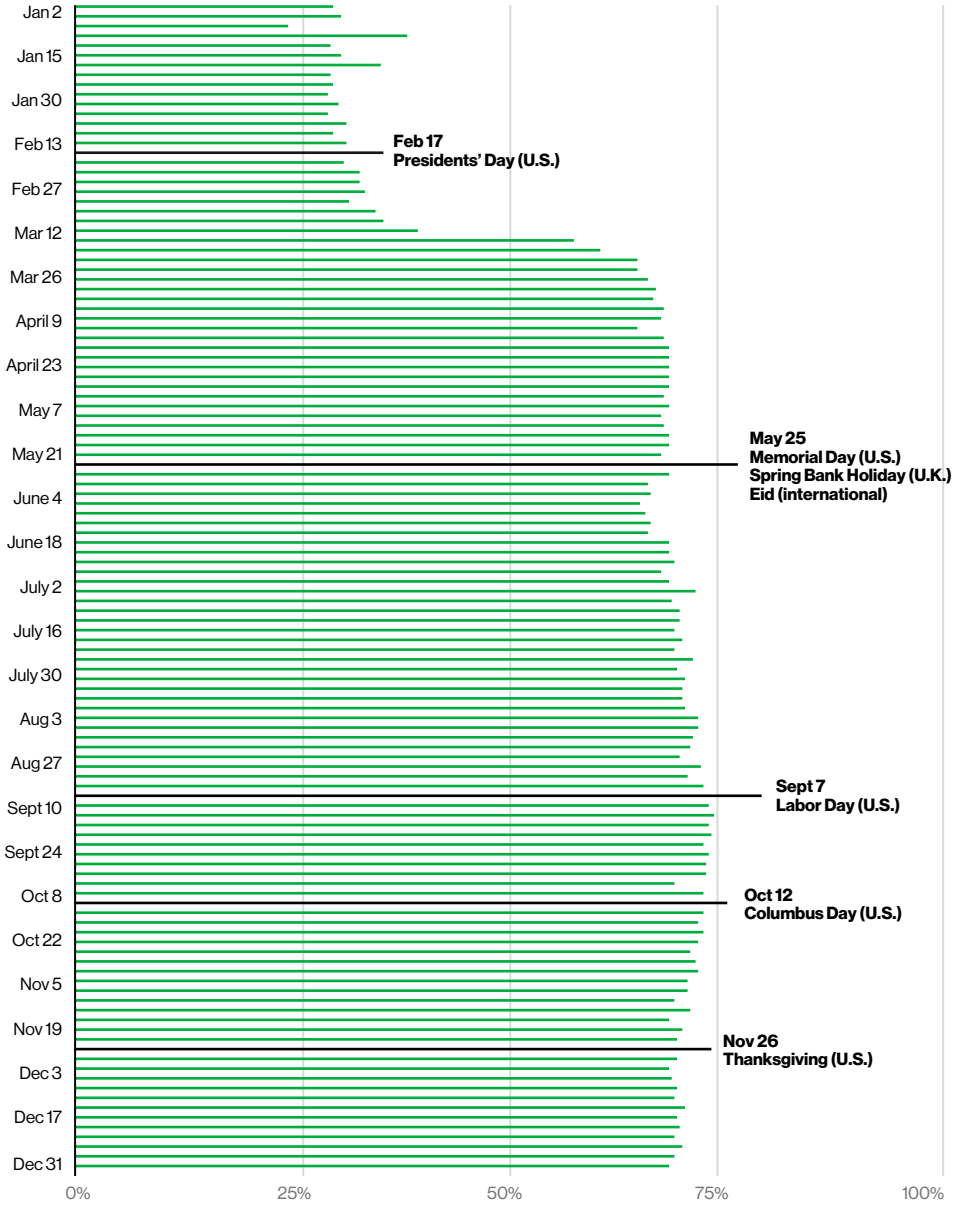


Figure 9. Split of workers, remote versus non-remote. Data from Netskope.[7]

6 Reuters, Reuters Next conference, January 2021.

7 Netskope, January 2021. Research was performed on anonymized usage data collected from a subset of Netskope Security Cloud platform customers (primarily North American) that had given permission for this use.

Our survey respondents reported similar numbers. Nearly four-fifths (79%) of organizations saw remote working increase. Overall, the share of remote workers grew from around a third (32%) of the average workforce before lockdowns began to nearly twice as many (62%) during lockdown.

We also asked respondents what they expected this proportion to be once COVID-19 is just a memory. A large majority (70%) of those that had seen remote working grow following the introduction of restrictions expected it to fall again afterward. However, 78% said that it would still remain higher than before lockdown. Overall, our respondents said that they expected the number of remote workers to settle at around half (49%).

Interestingly, the difference between small and medium-sized businesses (SMBs) and enterprises was quite small, just a few percentage points. The biggest difference was how much more capable larger companies were of adjusting operations to switch employees to working from home. SMBs increased home working by 22 pp, enterprises by 32 pp.

"Mobile devices were critical to maintaining business continuity during lockdown by enabling employees to stay productive from home. That explains the 26% increase in their use we saw in the first 100 days.

— Aaron Cockerill, Chief Strategy Officer, Lookout

Remote working peaked at nearly double, expected to settle at more than 50% up.

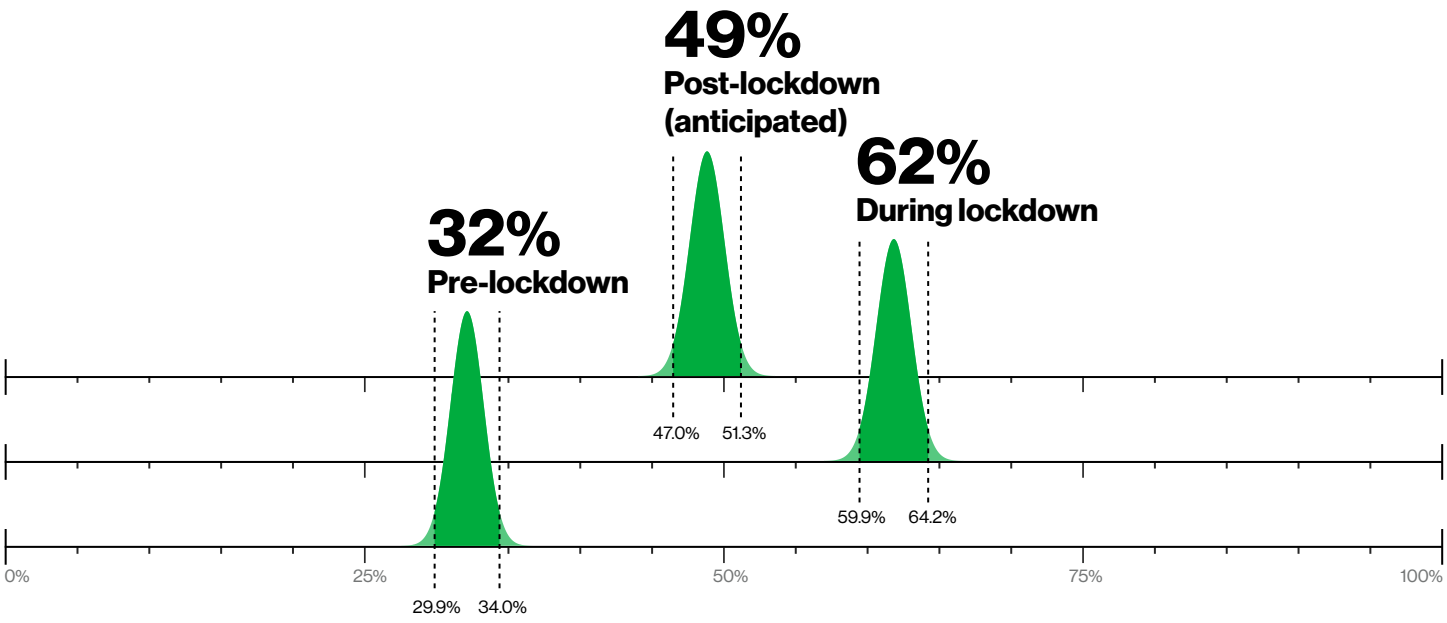


Figure 10. What proportion of your organization's staff work remotely, including from home? Include anybody that works outside the office more than 25 days per year. Lockdown refers to restrictions put in place in response to COVID-19. Dotted lines show 95% confidence intervals. [n=598]

This chart isn't meant as an homage to Joy Division—or the cover of the 2015 DBIR for you fans of our sister publication. Those of you with a knowledge of statistics will recognize these as confidence plots. The horizontal center of each curve shows the mean—32% in the pre-lockdown results. As our respondents are just a sample of all businesses, the actual average may be different; this is called sampling error. Statistically, we can say that the true number is within the two dotted lines with 95% confidence. In this analysis, the potential error is small, around just ±2 percentage points (pp).

89%

Eighty-nine percent of remote workers have encountered connectivity or poor user experience issues during the lockdown.[8]

Views on productivity when working from home vary by region.

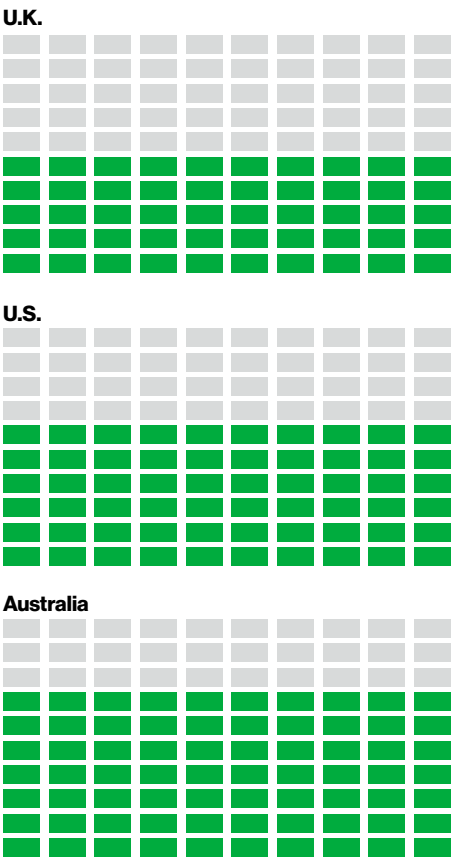


Figure 11. Is your workforce as productive working from home as when in the office? [n=598]

The productivity question

Historically, there have been many reasons why companies have been reluctant to let employees work from home. The main reason our respondents cited for not enabling more staff to work from home was the nature of their roles—either there was no demand for the role (for example, the store, restaurant or other site was closed) or the role couldn't be done remotely (for example, production line jobs and care workers).

Another reason has been that some leaders felt that staff couldn't—or wouldn't—be as productive working remotely. But attitudes are changing. Three-fifths (60%) of respondents to our survey said that the productivity of remote workers was at least as high as those onsite. And one in five (20%) said that it was significantly higher—and that was at a time of mass disruption, with many people using makeshift workstations and a large number of parents having to cope with challenges like remote schooling.

Enterprises (61%) were more likely to say that the productivity of remote workers was at least as good, compared to SMBs (54%). There was more variation by region. It's tempting to try to explain these numbers—and with U.S. and U.K. contributors, we had some interesting conversations—but we don't have the data to confirm any hypothesis.

These variances remind us about the dangers of averages. Working from home is much easier for some workers than others. For instance, the technology to create virtual call centers is well established, and companies with adaptable infrastructures were able to transition workers quickly. It's also worth noting that some companies were able to successfully empower staff to work from home, but not in their normal role. For instance, when its U.S. retail stores were forced to close, Verizon was able to retask staff to provide online support—which was seeing a huge growth in demand.

Not all roles are as easy to shift. Some industries, like manufacturing, tend to have more of these sorts of roles and so faced greater challenges.

Most companies think their workforce is at least as productive when working remotely.

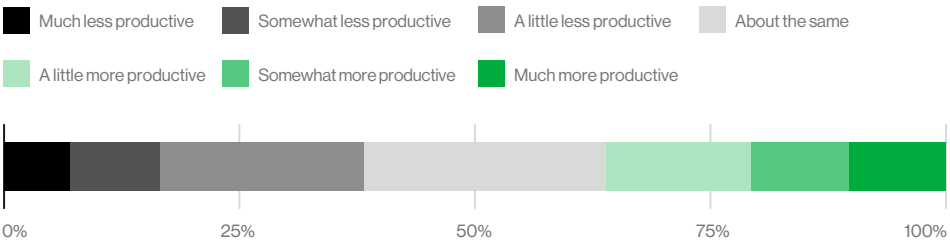


Figure 12. Is your workforce as productive working from home as when in the office? [n=598]

8 NetMotion, SDP report, June 2020. A survey of over 600 network and IT professionals across the U.S., the U.K. and Australia.

Lockdowns adversely affected security.

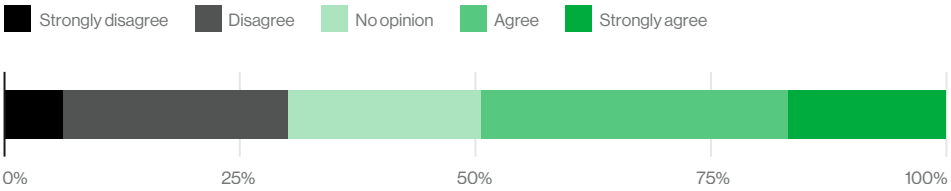


Figure 13. Changes to remote working practices made during lockdown adversely affected our security. [n=566]

Security and compliance issues prevented more people from working from home.

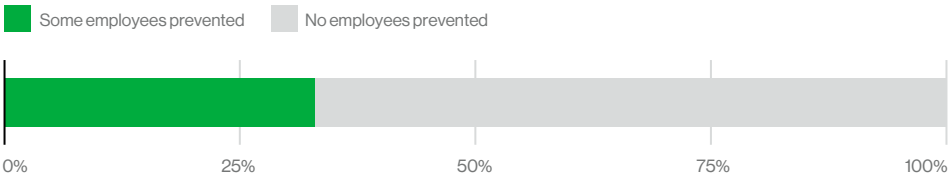


Figure 14. Why weren't more of your employees able to work from home during lockdown? Security/compliance issues.

Sales of MDM boomed.

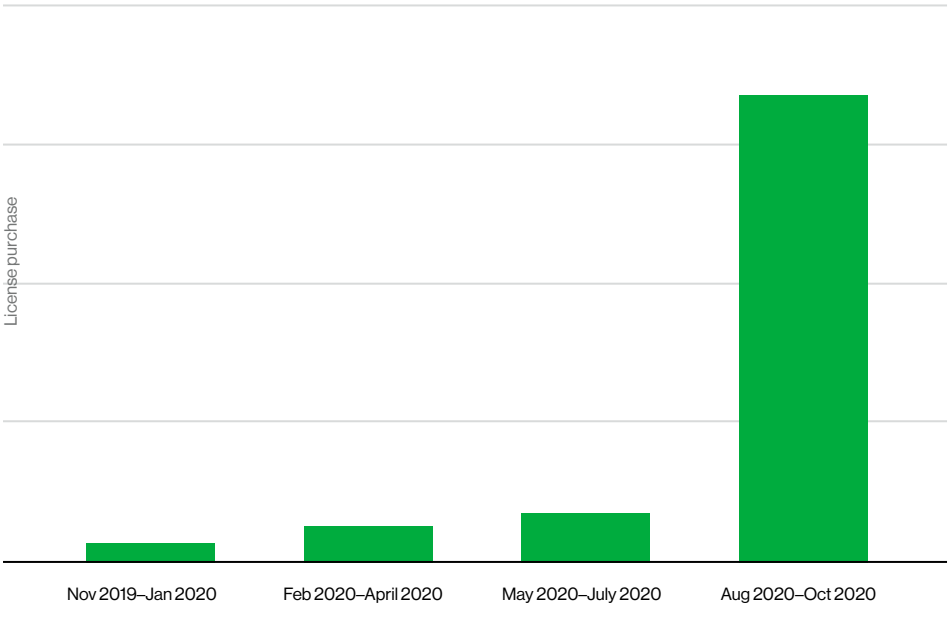


Figure 15. Volume of new license sales for Verizon MDM.

The security question

Nearly all (97%) security leaders consider remote workers to be exposed to more risk than office workers.[9] And almost half (49%) said that changes during lockdown conditions affected mobile security for the worse.

In fact, one in three (33%) respondents said that it wasn't possible to enable all the employees to work from home that they wanted to due to security or compliance issues.

One of the most obvious reactions to dealing with the security challenges of the increase in home workers was the increase in demand for mobile device management (MDM). Contributors to this report, like IBM, MobileIron and Wandera, all reported seeing an increase in new license sales, and Verizon saw an order-of-magnitude increase in purchases of its MDM solution.

"The number of requests for proposal (RFPs) for large enterprise mobile threat defense projects more than doubled from 2019 to 2020."

—Michael Covington, VP Product Strategy, Wandera[10]

According to NetMotion, 43% of companies experienced cybersecurity issues with remote workers in 2020.[11]

9 NetMotion, SDP report, June 2020. A survey of over 600 network and IT professionals across the U.S., the U.K. and Australia.
10 Michael Covington, statement, January 2021.
11 NetMotion, Experience Monitoring Report, November 2020. A survey of 500 IT professionals and 500 office workers now working remotely.

Working personas

Clearly, when it comes to where and how we work, the landscape has changed.

In the past, people have used terms like "remote working," "home working" and "flexible working" interchangeably. This fails to clearly describe the nature of the modern workforce and the nuances in behaviors and the threats they face.

We've identified seven types of employees. These fall into four categories based on the type of work they do and where the work is done. We've used these terms throughout this report for precision and clarity.

Non-remote workers

Employees that work inside a company-controlled environment, the perimeter, like an office, store or plant

Back office

Commuters

Office bound:
This includes a wide range of workers, from call center staff to lawyers. They might be required to work from the office, or chose to do so—not everybody likes or has the right conditions to work from home. These workers typically rely on a local area network (LAN) or wireless LAN (WLAN)—within the perimeter. They might work from home a few times a month.

Front of house

Tethered

Floor workers:
This category includes many roles in retail, hospitality, manufacturing, etc. These workers aren't fixed to a desk, but their location doesn't change much. They are more likely to use a specialized device. They will rarely use a network not controlled by the company.

Corridor warriors:
Employees that are never at their desks, but their roaming is mainly limited to one of the company's sites. They primarily use the company's WLAN.

Figure 16. Classification of types of workers.

Remote workers

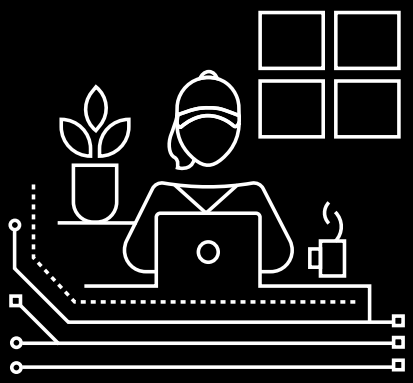
Employees that operate outside the perimeter, whether on the road or at home

Back office

Omniworkers

Home workers:
People based at home or who work from home a lot. This label can apply to a wide variety of roles. They typically use home Wi-Fi, perhaps with a virtual private network (VPN).

Flexible workers:
Employees that work from home a few days a week—there are all kinds of reasons why. They commonly use home Wi-Fi, perhaps with a VPN.



Front of house

Nomads

Road warriors:
These are the classic "remote workers": sales people, consultants, CxOs of big companies, etc. They need to be able to work from multiple locations and work on the move. They have complex requirements and use multiple types of networks. They are likely to need to use third-party Wi-Fi and cellular connectivity.

Field workers:
Another well-established category. It includes roles like service engineers. People in this group often need to use custom apps and work on the move—so cellular connectivity is key. Their primary device may be a customized or ruggedized device.

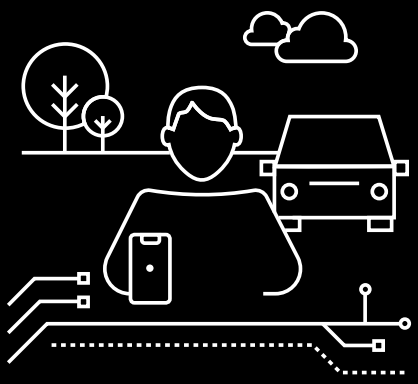


Figure 16 (continued). Classification of types of workers.

Bring your own.

Bring your own device (BYOD) was a very hot topic a few years ago. While vendors had introduced a number of variants (see below) prior to COVID-19, interest among organizations seemed to have waned. However, when restrictions were put in place to combat the pandemic, many companies relied heavily on employees using their own devices to maintain operations. More than one in three (36%) organizations opened up access to corporate resources and systems to employees using personal devices—that's on top of those that already allowed it.

Another factor driving increased interest in BYOD is the rise of the "gig economy." This isn't limited to delivery riders; roles like telesales and support can fit this model very well. Companies are increasingly using this approach to enable them to scale more quickly as demand ebbs and flows. Verizon's 2020 The Future of Work report found that about half (49%) of respondents thought that the pandemic had increased the importance of participating more actively in the gig economy in order to gain quick access to part-time and temporary workers.[12] Even if these workers don't have direct access to key business systems and data, attackers can exploit the access that they do have and then "move laterally" to more sensitive assets.

Models for employee device deployment

Name	Type of device	Who owns the device?	Who chooses the device?	Is personal use supported?
Bring your own PC (BYOPC)	PCs	Employee	Employee, sometimes with restrictions on suitable models	Personal use is primary
Bring your own device (BYOD)	Smartphones, tablets, PCs	Employee	Employee, sometimes with restrictions on suitable models	Personal use is primary
Choose your own device (CYOD)	Smartphones, tablets, PCs	Company	Employee, typically from a short list	Varies
Company owned, personally enabled (COPE)	Smartphones, tablets, PCs	Company	Company	Yes, typically in a sandbox
Company owned, business only (COBO)	Smartphones, tablets, PCs and custom-built, handheld or ruggedized devices	Company	Company	No

Figure 17. Bring-your-own models.

Lockdown drove many to look at BYOD and BYOPC models.

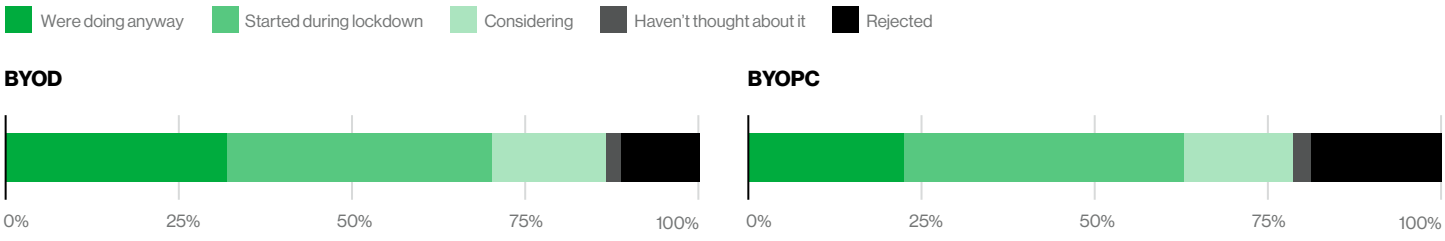


Figure 18. Which of the following have you adopted or considered? [n=598]

12 Verizon, The Future of Work, 2020, https://www.verizon.com/business/en-gb/solutions/digital-transformation/future-of-work/

The rise of the "Omniworker"

As we discussed earlier in this section, companies expected working from home to fall once restrictions were lifted, but to remain significantly higher than before – about 54% over pre-pandemic levels. Numerous reports have suggested that the majority of employees want to keep working from home at least some of the time.

Of those organizations that had adopted BYOD or BYOPC during lockdown, many (39% and 42% respectively) said that they anticipated continuing with it after restrictions related to COVID-19 were lifted.

This brings to mind the words of computing pioneer Admiral Grace Hopper: "It's easier to ask forgiveness than it is to get permission." Just as with the concept of home working, the uptake of bring-your-own programs had been hampered by ensconced attitudes. But now that the tanker (or should that be aircraft carrier?) has turned, it seems that many are happy to stick with their new course.

We anticipate that bring-your-own policies will be firmly back on the agenda in 2021.

Many companies plan to make temporary bring-your-own programs permanent.

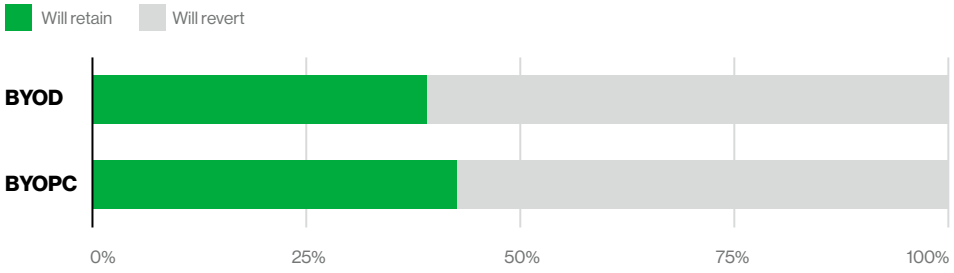


Figure 19. Which of the following have you adopted or considered? [n=598, 566]

97%▲

There was a 97% increase in personal use of managed devices.[13]

13 Netskope, Cloud and Threat Report, August 2020. Research was performed on anonymized usage data collected from a subset of Netskope Security Cloud platform customers (primarily North American) that had given permission for this use.

Securing BYOD/ BYOPC programs

Recommendations aligned with the NIST Cybersecurity Framework

These recommendation sections are structured around the five functions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a widely recognized model based on international standards and input from public- and private-sector organizations and academia. It provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework

Identify

As with any security topic, understanding the risks is a crucial first step. You should develop a detailed BYOD policy that clearly lists responsibilities.[14] This should tackle the tough questions, like does the organization have the right to remotely wipe (or seize) the device if a security threat is detected? But beware of being too draconian. A secure BYOD program relies on users feeling able to share concerns, not covering up potential issues. For the same reason, make sure that the policy is written in clear language and is easy to understand. This may involve translating it into local languages.

Ensure that all your employees understand their responsibilities when using their own devices for business purposes. This matters because people behave differently when using a personal device than when using a company-owned one. Differences could include letting a friend or family member use it, giving the login password to a third-party support or repair person, or simply visiting inappropriate sites.

Proofpoint found that the vast majority (90%) of people back up important files using a cloud-based storage service or an external drive.[14] While this could be good news from the perspective of business continuity—and thwarting ransomware attacks—it could be worrying in terms of IT having little insight or control over where sensitive data is stored. You should educate users on the dangers of storing corporate information locally on devices, especially ones not controlled by the organization.

Protect

Not all threats are malicious. Employees often increase risk unintentionally or even with the best of intentions. For example, a user might have their devices set up to automatically back up to the cloud. If that user then starts using a device for work purposes, this could not just pose an additional security risk but also contravene privacy regulations. Those who are new to remote working are likely to be less aware of such issues than experienced Omniworkers and Nomads.

Educate users on the importance of managing the permissions granted to apps. Users often aren't aware of how some permissions can be exploited for nefarious purposes.

There are a range of technical services, such as MDM, that can help remotely secure, manage and support personally owned devices. Some of these have a "container mode," which enables administrators to create an isolated area of the device to run corporate applications in. As well as giving increased control, this can also get around the potentially thorny issue of permission to wipe an employee-owned device.

Strong authentication is important on every device, but BYOD presents particular challenges. With personally owned devices, IT will have less control and visibility, so malware can be more of an issue. The compromise of credentials could lead to sensitive business applications and data being exposed. Consider using different credentials and giving devices not controlled by the company restricted access.

14 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.

Ensure that participants—especially former Commuters and others new to using personal devices for work—understand the importance of keeping both the operating system (OS) and apps up to date. And educate them on the dangers of malware and how to reduce the risks. Malware could obviate protections like containerization.

A zero trust approach is ideal for a BYOD program. It can reduce the reliance on end users making informed and security-conscious decisions. And it can improve user satisfaction and productivity as it automates many aspects of security protections, reducing the number of intrusions to the user's activities. See page 81 for more about zero trust.

Detect

BYOD devices should have all the standard security measures—such as mobile threat detection (MTD)—that you'd put on a company-owned and controlled device. An MDM solution can make managing a diverse fleet of devices much easier, including deploying applications, checking that patches have been installed and enabling remote wipe if a device is lost, stolen or compromised.

Endpoint detection and response (EDR) uses behavioral-based analysis to provide threat protection. A typical EDR solution consists of an app that sits on the device and gathers thousands of data points. These data points are automatically analyzed to detect threats and mitigate them. These solutions can also provide much greater visibility into the mobile fleet, providing valuable insight.

Consider implementing data loss prevention (DLP) to detect and block the exfiltration of information. But give users an authorized—and easy-to-use—means to share files outside the company to avoid putting them in a corner.

Respond

Many traditional security controls relied upon having a relatively homogeneous fleet of devices—the "bad old days" of everybody having the same brick phone and laptop. Most BYOD programs increase the variety of devices being used—in fact, many programs were introduced to answer demand for specific devices. This is likely to place increased demand on support, as there will be more operating systems to understand, more operating systems and app variants to patch, and more device-specific vulnerabilities to worry about. Make sure that your team is prepared for this, or you could be creating a security nightmare.

Ensure that staff members know what to do if a device is lost or stolen, or they spot something suspicious—which should be part of your general security policy, but it's worth reiterating here. Make sure that your employees feel comfortable reporting potential issues, as this can help identify attacks faster. Early detection can drastically reduce the damage caused, but, as anybody that's read the Verizon DBIR will know, it often doesn't happen.

Make it easy—it shouldn't be something people have to look up—and remember, the employee might not be able to access company systems when reporting an issue. Create a memorable external-facing email alias like security@companyname.com

Recover

Remember that employees may not have the cash to replace an expensive device and an insurance policy may take time to pay out. Make sure that you have some spare devices to loan to users to keep them productive while loss/theft issues are resolved.

Unlike devices bought by the company, the IT department may never get their hands on new devices under BYOD programs. Consider the time it may take to build a new device over a typical home broadband connection—apps like Microsoft 365 (formerly Microsoft Office 365) are a multiple gigabyte download. Provide users with advice on prioritizing the build process and how to use web-based options (such as Microsoft 365 Online) in the meantime.

MTD combined with unified endpoint management (UEM) can help bring devices that are out of compliance back into line through self-remediation.

Performing digital forensics on an employee-owned device can present many problems. Develop a clear policy in consultation with the legal department. Make sure that you have the processes and capability in place to carry out an investigation in line with the policy.

Small, but mighty

No longer a secondary device

Many employees now have access to much of the same valuable corporate data—customer lists, banking details, employees' personal data, billing information and much more—via their mobile devices as Commuters who sit in the office. This means that the compromise of a mobile device can now pose just as great a risk to your customer data, intellectual property and core systems.

The top compromised asset varieties for the 2020 DBIR time frame in cyber-espionage breaches were desktop or laptop (88%), mobile phone (14%), and web application (10%).[15]

The majority (71%) of respondents said that mobile devices are "critical to their business," which we defined as an answer of 8 or higher on our 10-point scale. And over a third (34%) scored the importance of mobile devices at the maximum 10.

That makes them a risk.

Three-fifths (60%) of respondents said that mobile devices are their company's biggest IT security threat. Of those who didn't agree with that statement, the vast majority (85%) said that mobile devices are at least as vulnerable as other IT systems. And close to a third (31%) of all respondents agreed that mobile device threats were growing faster than other threats.

Forty-four percent rated the risk as significant or high. A further 42% rated it moderate. That picture varies by industry, with sectors like professional services and financial services expressing much greater concern.

Mobile devices are critical to business operations.

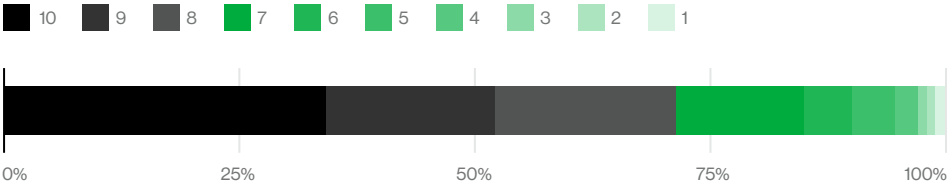


Figure 20. How critical are mobile devices to the smooth running of your organization? 1 = not at all, 10 = extremely [n=598]

There's widespread recognition of the risk from mobile device threats.

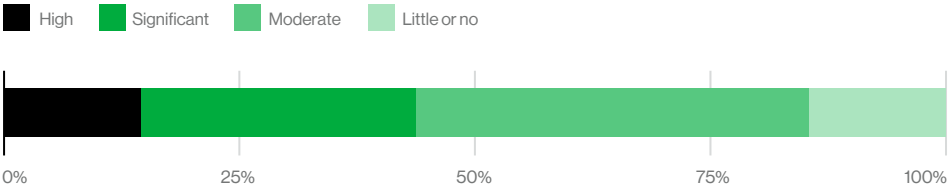


Figure 21. How would you assess your organization's risk from mobile device threats? Consider any security risk stemming from the use of smartphones, tablets or laptops using mobile data. [n=590]

15 Verizon, 2020 Data Breach Investigations Report, May 2020. [n=113]

Lockdowns adversely affected security.

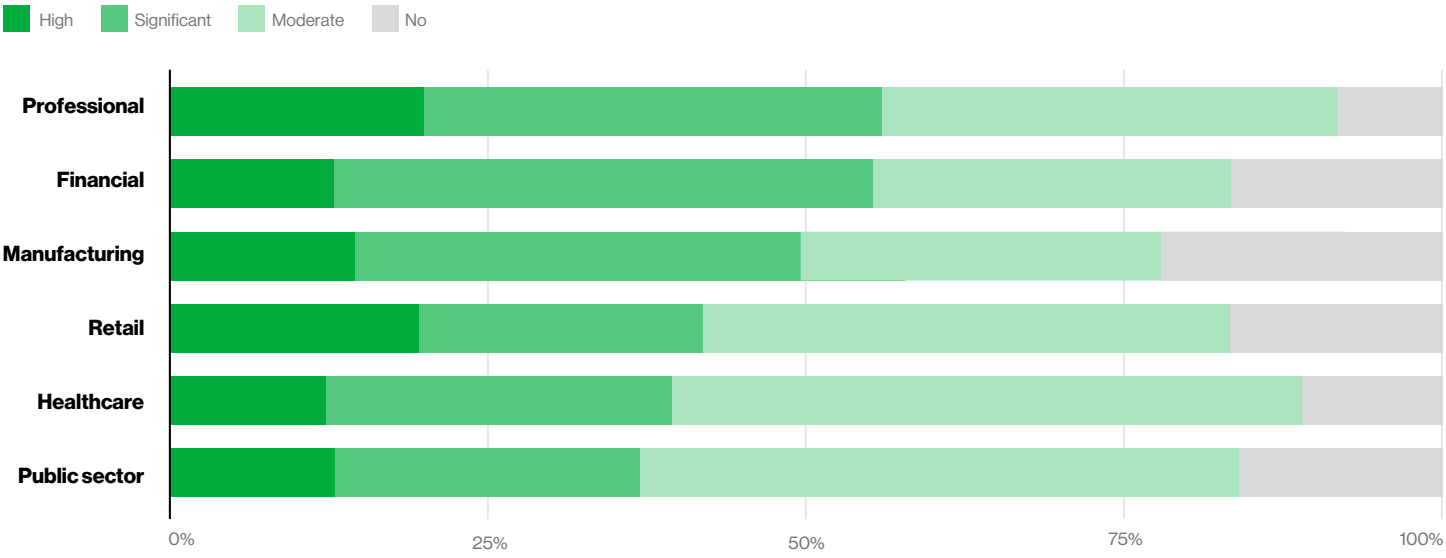


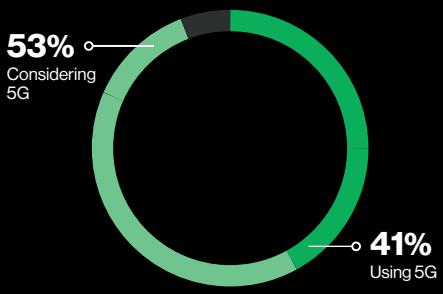
Figure 22. How would you assess your organization's risk from mobile device threats? Consider any security risk stemming from the use of smartphones, tablets or laptops using mobile data. [n=508]

Find out more.

Learn more about mobile device security threats in your industry in our set of industry-specific companion reports:

- **Financial services:** enterprise.verizon.com/msi-financial-services
- **Healthcare:** enterprise.verizon.com/msi-healthcare
- **Retail:** enterprise.verizon.com/msi-retail
- **Manufacturing:** enterprise.verizon.com/msi-manufacturing
- **Public sector:** enterprise.verizon.com/msi-public-sector

5G and multi-access edge computing



Forty-one percent of respondents said that their organization had already begun using 5G and a further 53% said that they are actively considering it.

In the two preceding editions of this report, we've looked at the additional security features built into 5G. Since we first wrote about it, 5G technology has gone from our test facilities to being available to millions of users: Verizon 5G is available in over 2,700 cities across the U.S. and private 5G services are being rolled out around the world.

Back in the days of 3G, watching video on your mobile phone was doable, but it wasn't exactly a great experience. Today, we take for granted being able to stream high-def video and do a million other things on our phones.

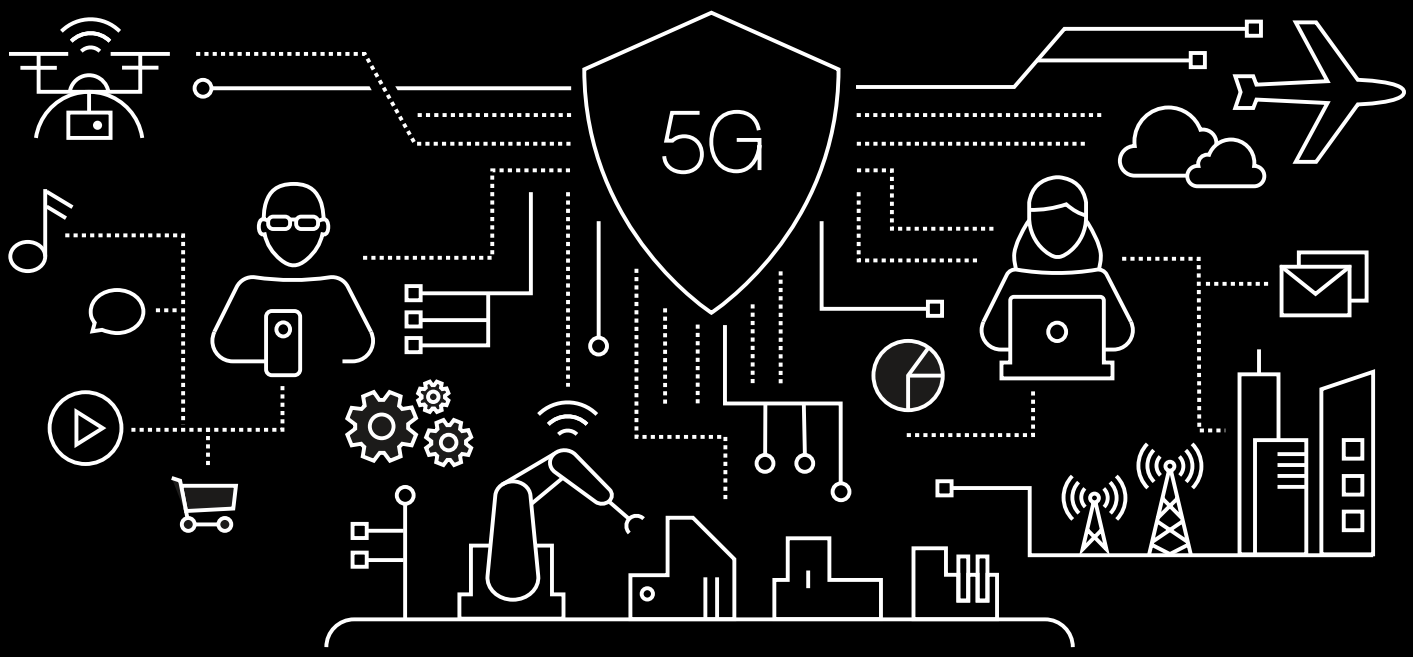
We'll probably look back on the launch of 5G in a similar way. And—like the transition from 3G to 4G, as well as making the doable better—5G will make entirely new things possible. Very soon, it will seem normal that everything is connected and intelligent. And in 10 years' time—that's how long 4G has been around—the world will be barely recognizable.

5G has been developed to support technologies that weren't really on the agenda when 4G was developed, like smart devices, augmented reality and artificial intelligence/machine learning (AI/ML) apps. It is able to deliver ultralow-latency, high-bandwidth connectivity reliably to a huge number of devices.

Together with important advances in edge computing, 5G offers fast, affordable connectivity for a massive number of devices—single-digit millisecond latency and up to 1,000,000 devices per square-kilometer. That's game-changing. It's light-years ahead of anything that's gone before in being able to exchange rich real-time data.

The potential applications are mind-boggling. Today, robots mainly do repetitive tasks. With 5G and edge computing, we'll see intelligent robots take on much more complex and interactive tasks. And cobotics, when robots and people collaborate, will take human capabilities to new levels. We'll also see digital twins and mirror worlds—virtual replicas of real-world environments—enable companies to optimize their operations and weigh the effect of changes before making them. 5G and edge computing will also facilitate intelligent video applications. This will enable automated quality control and many more game-changing applications in manufacturing and beyond. In retail, there's no shortage of ways to deliver magical experiences for shoppers, like extended-reality changing rooms and intelligent virtual assistants. The possibilities are almost endless.

The built-in security improvements help, but otherwise securing personal 5G devices, like phones and tablets, is very similar to securing their 4G, and even 3G, cousins. However, these new applications, often using entirely automated devices, present new challenges. Also, as these new uses generate richer data, attackers will find new ways to exploit it.



The simple solution would be to "wait and see," but the potential benefits of 5G-enabled applications are too great for companies to let their competitors get the upper hand. It's vital that companies choose partners that have the expertise and experience required to build security into solutions from the ground up. This includes physically hardening devices, implementing device authentication, encrypting data in transit, patching and testing for vulnerabilities, and managing network security.

Find out more.

Learn more about securing traffic over 5G.

https://enterprise.verizon.com/resources/whitepapers/2020/tech-target-whitepaper-3-securing-5g-network-traffic.pdf

"CISOs should consider adopting 5G devices that provide always connected and secure frameworks to the cloud. These enable the workforce to be efficient from anywhere, with advanced security features, such as platform intelligence and zero trust, that help protect against potential risks."

—Miguel Nunes,
Senior Director Product Management,
Qualcomm

The threats are real. 03

Despite everything that's at stake, many businesses still sacrificed the security of mobile devices—and those that did were more likely to have been compromised. Expediency, including responding to the COVID-19 crisis, remains the primary reason for cutting corners.

The number compromised was down.

While the share of companies aware that they had suffered a mobile-related compromise was down, the severity of compromises remained high.

Just 12% of those that had suffered a compromise, less than one in eight, said that the consequences were minor. Over half (53%) said that the consequences were major. That's actually lower than in the 2020 report, where 66% described the impact as major. But the percentage that said that the event had lasting repercussions was very similar, 33% in 2021 and 36% in 2020.

There was significant variation in the perceived severity of mobile-related compromises when broken down by industry.

Given that respondents rated the impact of compromises lower, it's not surprising that they also thought that they were easier to remediate. But despite the improvement here, almost a third (32%) described the measures needed to put things right as "difficult and expensive."

Almost a third (32%, down from 37% in our 2020 report) of respondents said that the compromise that they experienced was difficult and expensive to remediate.

But there is no room for complacency.

Companies sacrificing security/experiencing a mobile-related compromise

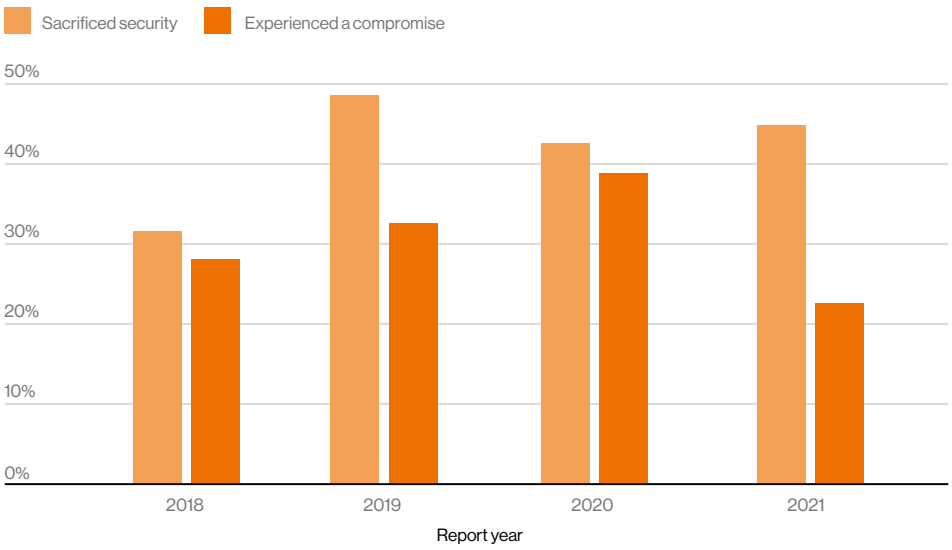


Figure 23. Has your organization experienced a security compromise involving mobile/IoT devices during the past year? Has your organization ever sacrificed the security of mobile devices (including IoT devices) to "get the job done" (e.g., meet a deadline or productivity targets)? [n=601, 671, 876, 856]

The severity of consequences remained high.

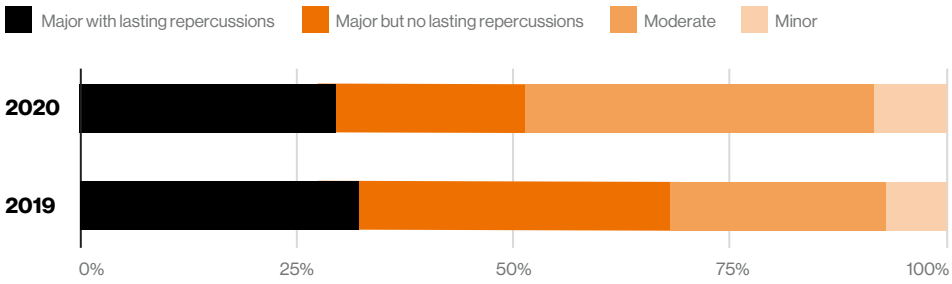


Figure 24. How serious was the impact of the security compromise(s)? [n=246, 134]

The share of compromises seen as major with lasting repercussions varied by industry.

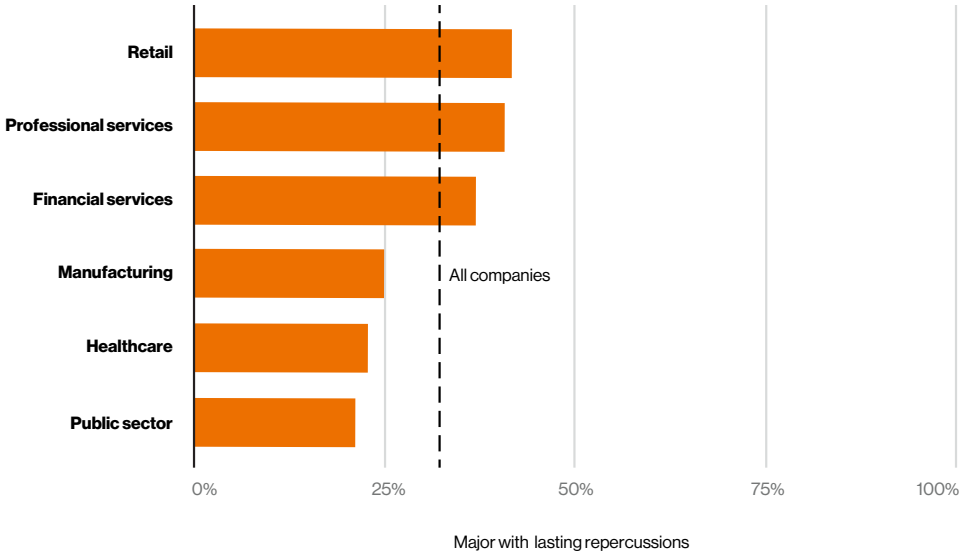


Figure 25. How serious was the impact of the security compromise(s)? [n=134]

Find out more.

Learn more about mobile device security threats in your industry in our set of industry-specific companion reports:

- Financial services
- Healthcare
- Retail
- Manufacturing
- Public sector

The scale of remediation required varied but was often high.

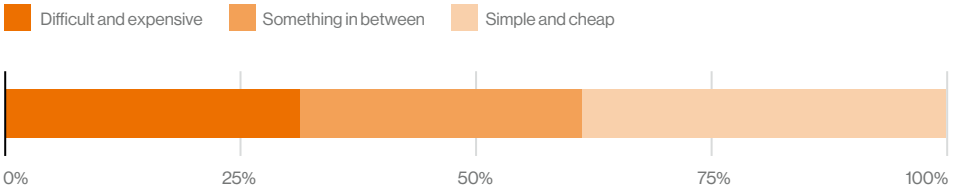
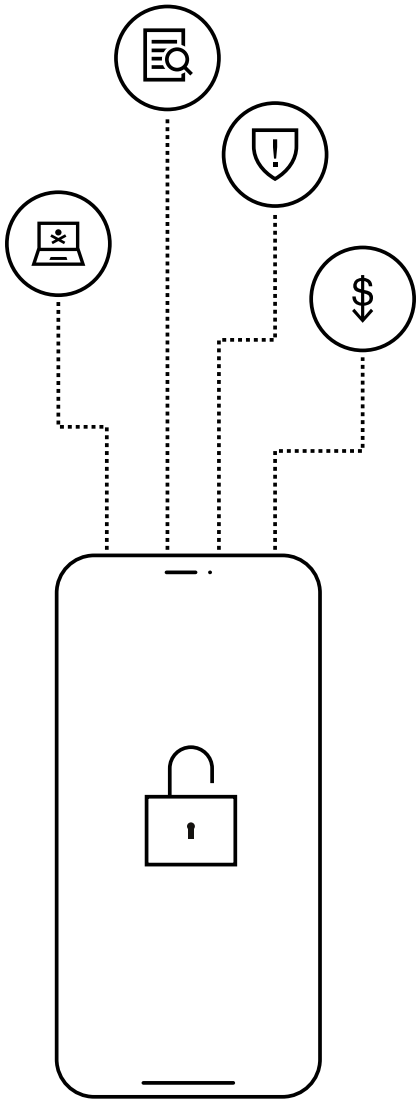


Figure 26. How would you describe the actions required to remediate the security compromise(s)? [n=133]



It's more than data that's at risk.

If you're reading this report, and obviously you are, it's highly likely that you have an above-average appreciation of cybersecurity risks. Way above average.

To a lay person, security compromise and data breach may be synonymous, but you know better. The exposure of sensitive data was the most common consequence of a compromise among our respondents, but it wasn't the only one. Two-fifths (40%) said that cloud apps/systems had been compromised, and nearly as many (37%) said that credentials had been.

Mobile device compromises affected more than data.

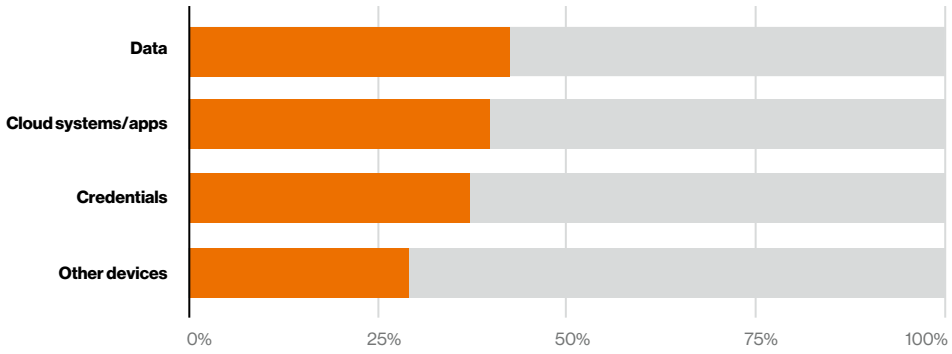


Figure 27. Which of the following consequences did your organization experience as a result of that security compromise? [n=134]

These were the IT consequences. Nearly all (96%) of the respondents that had experienced a mobile-related compromise faced business consequences. This includes nearly a quarter (23%) that said they had directly lost business as a result of the compromise.

The impact of compromises went beyond IT.

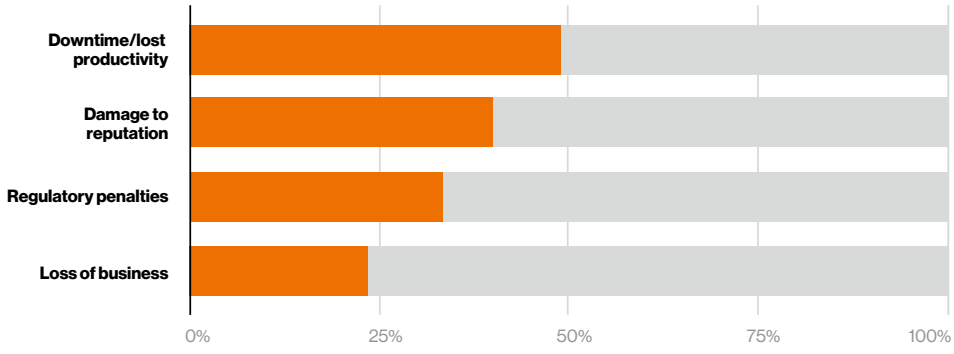


Figure 28. Which of the following consequences did your organization experience as a result of that security compromise? [n=134]

The pressure to sacrifice security

Almost half of respondents admitted that their company had knowingly cut corners on mobile device security. That's an increase from our 2020 report when the figure was 46%. The proportion rises to two-thirds (67%) in our IoT sample.

And of those remaining, 38% (27% IoT) came under pressure to do so. Another way of looking at this is that 68% came under pressure to cut corners and 72% of those succumbed.

The reasons for cutting corners were numerous, but responding to the COVID-19 crisis was the most common (48%). Organizations were forced to turn Commuters, along with many of the Tethered redirected to other roles, into Omniworkers almost overnight. And many struggled to maintain security standards.

Most respondents came under pressure to sacrifice mobile device security.

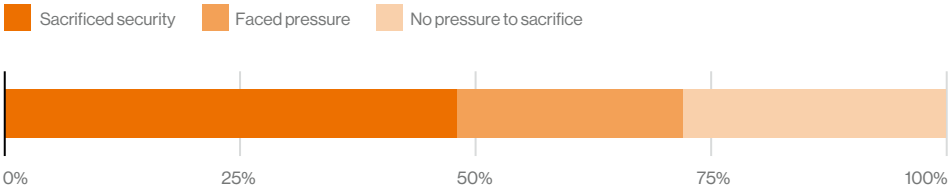


Figure 29. Have you ever sacrificed the security of mobile devices (including IoT devices) to "get the job done" (e.g., meet a deadline or hit productivity targets)? Have you ever come under pressure to relax policies or sacrifice the security of mobile devices? [n=586, 297]

Companies' reasons cited for sacrificing mobile device security.

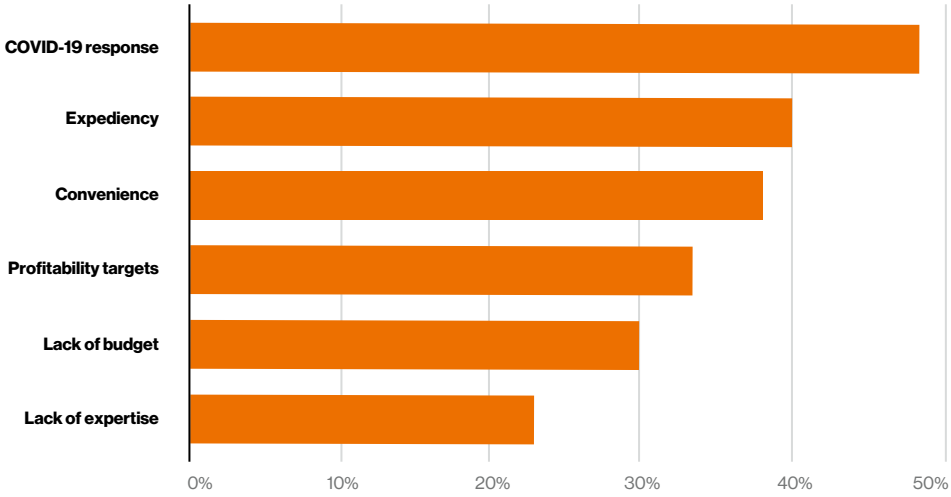


Figure 30. What was behind the pressure to make this compromise? Examples were given for "Expediency" (pressure from management to get product/service to market quickly) and "Convenience" (easier to go around company policy). [n=289]

What do companies sacrifice security for?

As we discussed earlier, expediency and convenience were the main justifications cited for sacrificing security, with COVID-19 making a special guest appearance in our 2020 dataset. In our latest survey, we asked respondents not just why they sacrificed security, but also what for. And the results weren't what we expected.

Unsurprisingly, respondents overwhelmingly said that they prioritize security over usability.

When it comes to balancing security and manageability, there was a much more even spread. That might lead you to expect that manageability would comfortably outscore usability when the two were put head to head. But actually, respondents were more likely to say they favored usability.

This was an interesting exercise, but, in reality, security, manageability and usability go hand in hand. If security measures are too onerous on users, they will look for workarounds. If security measures aren't manageable—or make other aspects of IT less manageable—IT may struggle to ensure compliance and consistency.

Companies put security before usability.

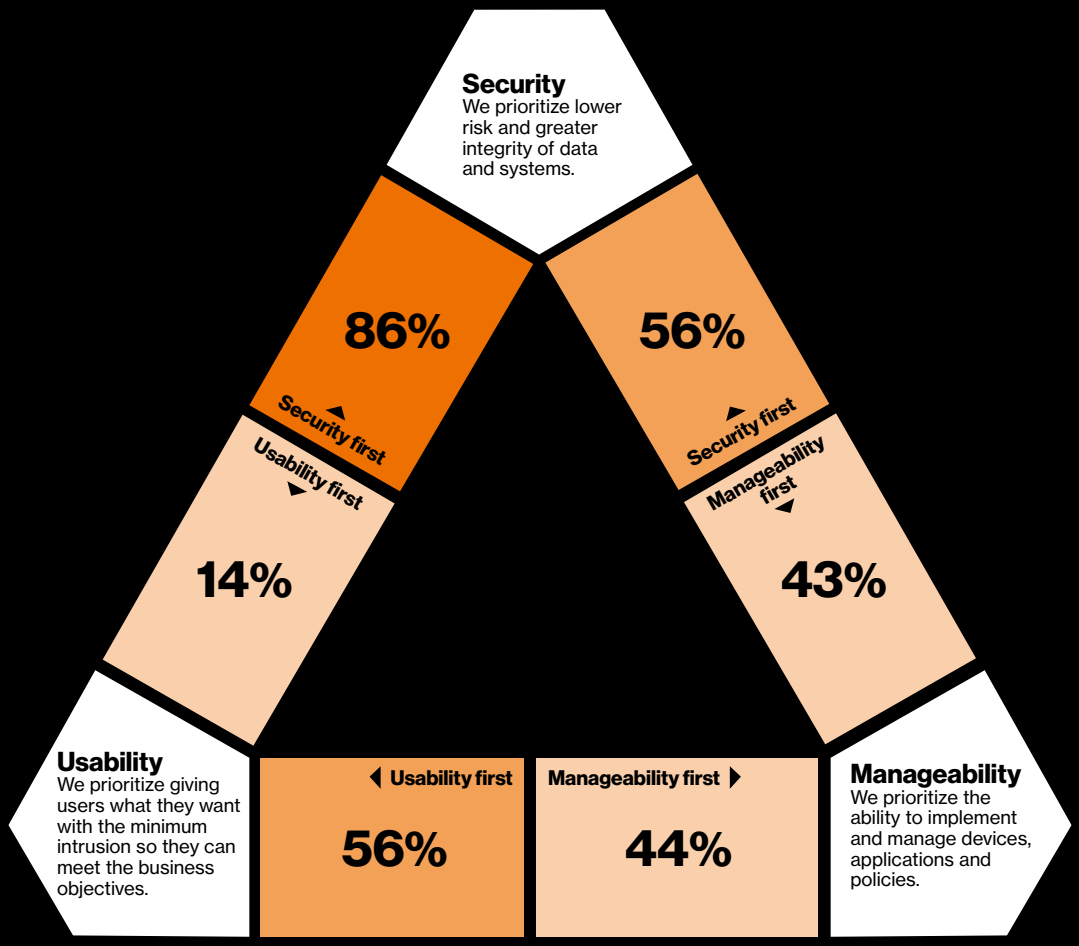


Figure 31. When making security-related decisions, how do you balance usability and security, security and manageability, manageability and usability? [n=856]

Shadow IT

Gartner defines shadow IT as "IT devices, software and services outside the ownership or control of IT organizations."[16] It came to prominence several years back when cloud-based services that could be bought (relatively) inexpensively with a credit card entered widespread use. But cloud isn't the only driver behind the growth of shadow IT.

Mobile device management was much easier in the days when companies issued a standard model of device—often a BlackBerry—and apps were extremely limited. Today, users expect to be able to use the devices and apps that they like and think make them most productive.

The majority of respondents (85%) said that when faced with a choice between security and usability, security comes first. This can create a conflict with users. It's little wonder then that five out of six respondents said that they are worried about the emergence of shadow IT.

With so many companies opening up systems to personal devices and relaxing restrictions on apps to cope with the effects of COVID-19, shadow IT may be more of an issue in the coming years. Once a freedom is given, it can be very difficult to take back without creating much resentment.

Respondents were worried about the rise of "shadow IT."

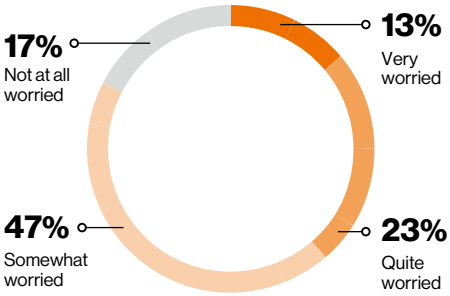
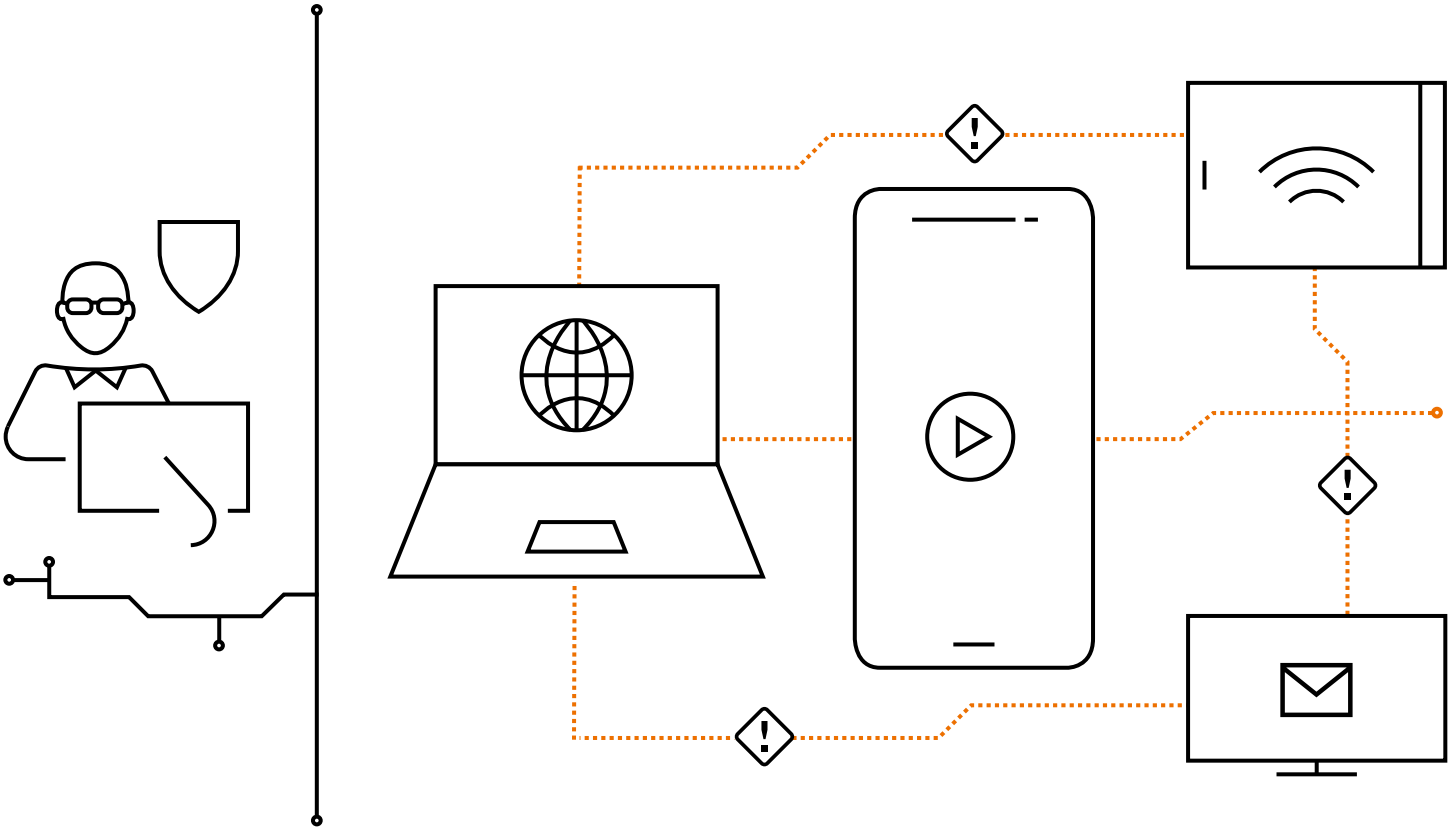


Figure 32. Are you worried about the emergence of "shadow IT," lines of business or business units making their own IT purchases or app choices? [n=598]



16 Gartner, Glossary: Shadow IT.

The mobile threat landscape

04

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

In this section:

04.1 People and behaviors

04.2 Apps

04.3 Devices and things

04.4 Networks and cloud

In this year's report, we've extended our framework to incorporate the stories around cloud and other topics we've added to this report over the past couple of editions.

Pandemic-related spike

A 2020 Check Point report found that COVID-19-related phishing and malware attacks increased from fewer than 5,000 per week in February 2020 to more than 200,000 per week by late April. In May and June, as countries started to ease lockdowns, threat actors stepped up their non-COVID-19-related exploits. This resulted in a 34% increase in all types of cyberattacks globally at the end of June compared to March and April.[17]

17 Check Point, Cyber Attack Trends: 2020 Mid-year Report, July 2020. Analysis of customer data gathered between March 2020 and April 2020.

04.1 People and behaviors

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

Quick takes

- Over half (54%) of companies that had experienced a mobile-related security breach attributed it, at least in part, to user behavior, such as falling for a phishing attack, installing unsanctioned apps or making unintentional errors
- Lookout saw a 364% increase in the number of mobile phishing attempts in 2020 versus 2019[18]
- Netskope Threat Labs found a 600% increase in the number of visits to websites hosting adult content[19]
- In a NetMotion research study, only a third (36%) of organizations said they were satisfied with their current level of visibility into mobile devices[20]
- Mobile device users are 26 times more likely to click on a phishing link than they are to encounter malware[21]

Problem in chair, not in computer

Almost half (49%) of respondents in our survey that had experienced a mobile-related security compromise said that user behavior was a contributing factor. This included falling for phishing attacks, installing unsanctioned apps or making unintentional errors.

Nearly half of those that were compromised blamed user behavior.

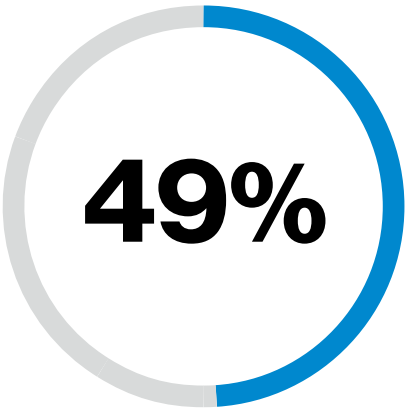


Figure 33. Which of the following contributed to this/these security compromise(s)? [n=134]

18 Lookout, analysis of all enterprise users covering January 2019 to December 2020.
19 Netskope. analysis based on anonymized data collected from the Netskope Security Cloud platform across millions of users from January 1, 2020, through June 30, 2020.
20 NetMotion, SDP report, June 2020. A survey of over 600 network and IT professionals across the U.S., the U.K. and Australia.
21 Wandera, analysis of data from entire global customer base between January 1, 2020, and December 31, 2020.

VAPs not VIPs[22]

Attackers are pretty adept at innovation—mal-innovation was a focus of our 2020 edition—and the threat landscape is constantly evolving. But device manufacturers and OS developers have taken great strides in hardening devices, too. Faced with more obstacles to their efforts, "wetware"[23] is an attractive weak spot for attackers.

These attacks focus on people and identities rather than infrastructure, making it more important than ever to identify those users in an organization who represent the greatest risk. According to Proofpoint, "very attacked people" (VAPs) represent significant areas of risk for organizations. They tend to be either easily discovered identities or targets of opportunity like shared public accounts.[24]

Of the VAPs identified by Proofpoint, 36% of the associated identities could be found on corporate websites, social media, publications and other readily accessible sources. VAPs are not necessarily high-profile individuals. For good reason, few CEOs and other C-level executives make their email addresses and other information openly available—only 7% of executive emails could be found online.[25]

Phishing

Yawn. Yes, phishing again.

Despite being a regular feature in reports like this and discussions among IT security folks, many staff still don't understand what phishing is. Proofpoint found that just 61% of employees were able to select the correct definition. Two-thirds (66%) of German respondents knew what it was, and less than half (49%) of American respondents got it right.[26]

And if they don't understand what phishing is, they are unlikely to be able to defend themselves—and hence the organization—effectively.[27] That helps to explain why phishing remains a common, and effective, type of attack.

Many employees don't even know what phishing is.

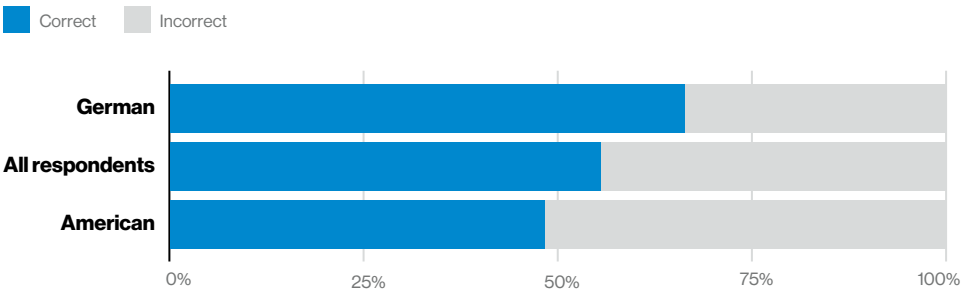


Figure 34. Employees able to correctly define "phishing" by country. Data from Proofpoint.[28]

22 Proofpoint, Human Factor Report, August 2019, based on analysis of 18 months of data from Proofpoint's global customer base.
23 A slang term that is used to describe the human component of IT systems.
24 Proofpoint, Human Factor Report, August 2019, based on analysis of 18 months of data from Proofpoint's global customer base.
25 Ibid.
26 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
27 Ibid.
28 Ibid.

Enterprise phishing encounters were up year-on-year.

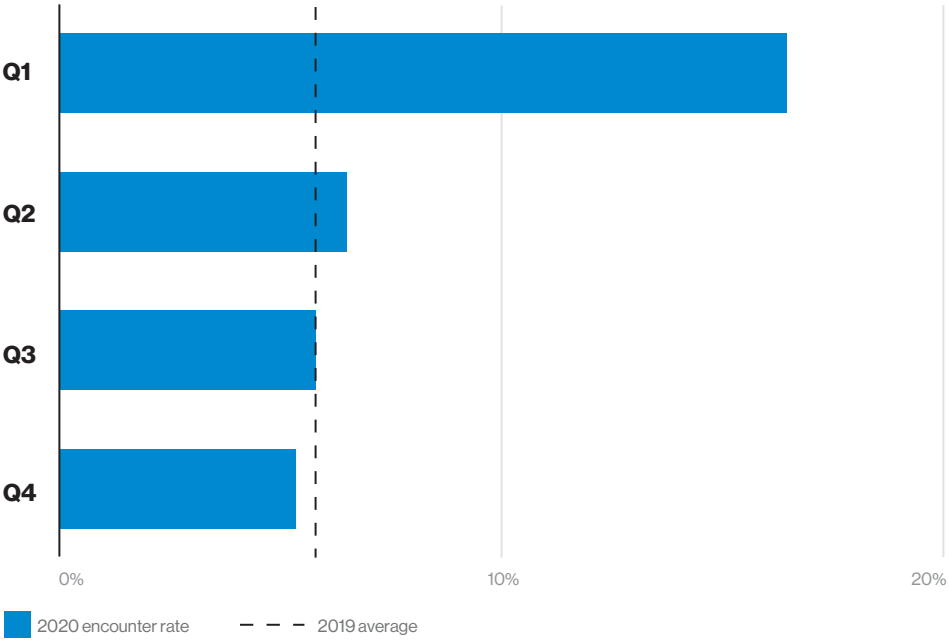


Figure 35. Phishing encounter rate. Data from Lookout.[29]

More users were subject to phishing attacks.

	2018	2019	2020	CAGR
Percent of organizations	15.1%	36.5%	35.9%	+154%
Percent of devices	0.4%	3.5%	4.4%	+332%

Figure 36. Incidence of phishing attacks. Data from Wandera.[31]

While the increase in enterprise phishing rates is worrying, the increase in mobile phishing rates is significantly more alarming.

364%▲

Lookout saw a 364% increase in the number of mobile phishing attempts in 2020 versus 2019.[32]

26x

Wandera has also seen a big jump in mobile phishing incidents. In fact, mobile users are 26 times more likely to click on a phishing link than they are to encounter malware, one of the other most common attack types.[33] Over a third (56%) of organizations and 8% of users encountered a phishing attack on their mobile device between September 2019 and August 2020.[34]

29 Lookout, analysis of all enterprise users covering January 2019 to December 2020.
30 Compound annual growth rate.
31 Wandera, all corporate users, full calendar year given.
32 Lookout, analysis of all enterprise users covering January 2019 to December 2020.
33 Wandera, analysis of data from all corporate customers gathered between September 2019 and August 2020.
34 Ibid.

Evolution of phishing

As tools to block email threats evolve, hackers are continually innovating. They are developing new techniques to evade detection and lure hapless users into handing over money, surrendering valuable information or unwittingly installing malware.

"We have seen attackers obtain credentials to email accounts, study the victim for weeks and when the time is right, craft a targeting attack against partners and customers to steal money. Over the last two years, this attack has spiked with the increased use of software-as-a-service-based email solutions."

—Dan Wiley, Check Point[35]

Top 20 most impersonated brands

Brand	Category
1. **Apple**	Tech
2. **PayPal**	Bank/financial
3. **Microsoft**	Tech
4. **Office 365**	Tech
5. **UK Government**	Government
6. **Amazon**	Retail
7. **Google**	Tech
8. **Samsung**	Tech
9. **Wells Fargo**	Bank/financial
10. **Visa**	Bank/financial
11. **RuneScape**	Leisure
12. **Facebook**	Social
13. **Skype**	Tech
14. **Adobe**	Tech
15. **Instagram**	Social
16. **Intuit**	Bank/financial
17. **Fox News**	News
18. **Chase**	Bank/financial
19. **American Express**	Bank/financial
20. **Capital One**	Bank/financial

Figure 37 (above). Brands most frequently used in phishing attacks. Data from Wandera.[35]

Figure 38 (right). Types of phishing attacks.

35 Dan Wiley, Head of Incident Response, Check Point.
36 Wandera. All corporate customers, full year 2020.

Phishing campaigns can be broken into four distinct types:

Scam	Sadly, that email from a widow in a distant country who wants to deposit hundreds of millions of dollars into your bank account is probably a scam. We can laugh about it, but emails like this are still common. Fortunately, email scanning systems catch most of the most obvious examples, but some still get through. **Common attack variants include:** • The executor tasked with fulfilling a legacy • The billionaire that wants to share their wealth • The relative who is trapped overseas and needs cash to get home • The fake invoice/penalty charge
Brand impersonation	Impersonating a bank or service provider is another attacker favorite. This type of attack is popular in smishing attacks—phishing attacks by short message service (SMS). **Common variants include:** • "A new payee has been set up; if that wasn't you, click here" • "Your account has been suspended due to suspicious activity, click here to reactivate/secure your account" Banks and big tech firms are among hackers' favorites, but they aren't alone—see Figure 37 for the latest "Top 20."
Extortion	Not all phishing emails are intended to fool the recipient. Some are much more direct. A common tactic is "sextortion." **Common variants include:** "I've got bad news for you. Weeks ago I installed spyware on your computer and have been watching you have fun. Send bitcoin or I will share the recordings with everybody in your address book."
Business email compromise	Business email compromise (BEC) attacks—also known as email account compromise (EAC) or CEO fraud—have grown rapidly in recent years. This type of phishing attack is typically highly targeted and pays big when successful. **Common variants include:** • The urgent payment—"This is the CEO, I need you to..." • The payroll diversion—"Please send future salary payments to..." • The supplier update—"Please send future payments to..." See the section on BEC attacks on page 44.

The COVID-19 effect

The spike in enterprise phishing can largely be explained by campaigns exploiting uncertainty and nervousness around COVID-19. This shows that actors can act extremely quickly, and that they are prepared to take advantage of anything to phish victims.[37]

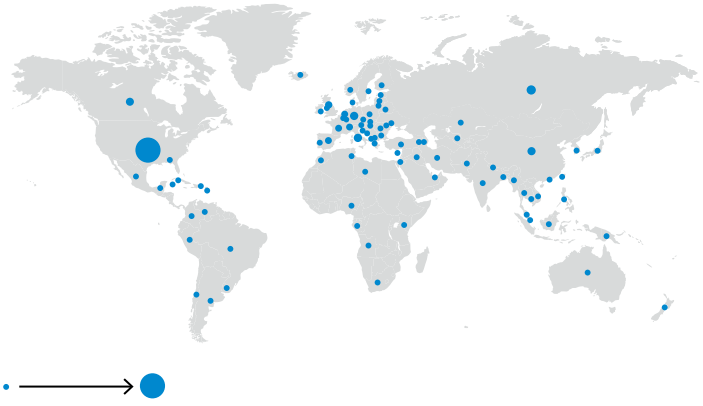
> **"We know that cybercriminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the Coronavirus outbreak."**
>
> —Paul Chichester, Director of Operations, National Cyber Security Centre (NCSC)[38]

Soon after countries around the world began implementing COVID-19 lockdowns, Check Point observed a spike in registrations of domain names, including "Zoom," a common "freemium" video conferencing application. Registrations were already high, at about 116 per week; then, in the final week of March, they reached 425.[39] It's unlikely to be a coincidence that this was when many people were looking for a quick solution to communicating while stuck at home.

About 1.2 million of the domains registered between March 9, 2020, and April 26, 2020, a period of seven weeks, included "coronavirus," "covid," another COVID-19-related term or a punycode[40] variation of one of these. Of course, many of these will be legitimate sources of information. Some will be for more traditional scams, people just looking to take advantage of the situation or examples of cybersquatting. But about 7% (over 86,000) were classified as "high-risk" or "malicious." This means that they were found to already be connected to command and control (C2), phishing or malware attacks.

But Wandera saw a sizable number of users visiting unsafe COVID-19-related domains throughout 2020.

COVID-19-related domains were registered worldwide.*



Size of circle relates to number of registrations.

Figure 39. Registrations of COVID-19-related domains categorized as "high risk" or "malicious." Data from the Unit 42 research team at Palo Alto Networks.[41] Size of circle relates to number of registrations.

*The most COVID-19-related domains were registered in the U.S., reflecting registrations in general.

Many users were lured into visiting unsafe COVID-19-related domains.

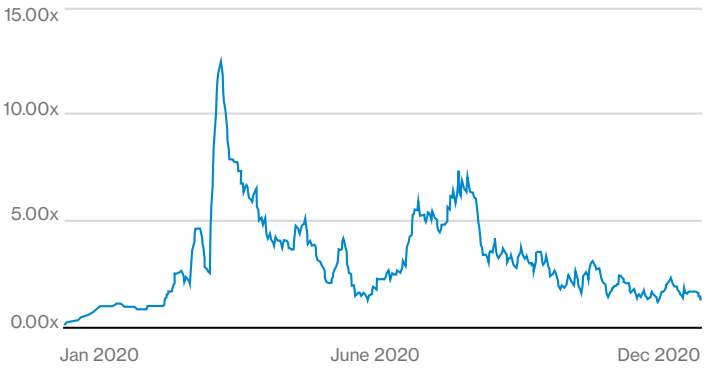
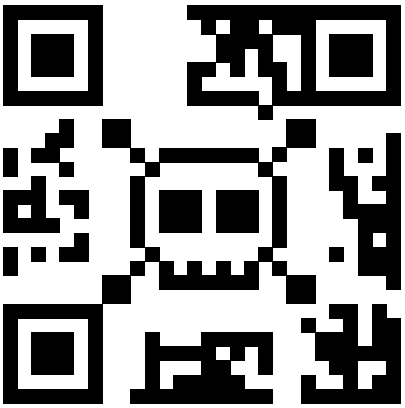
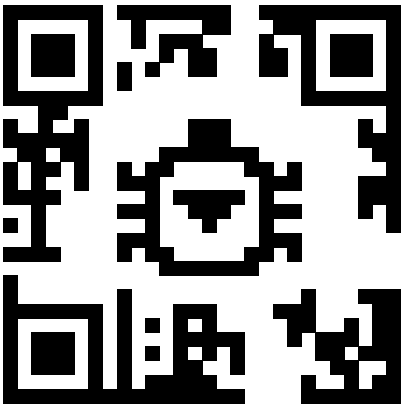


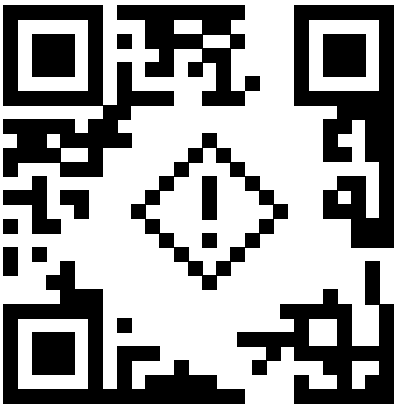
Figure 40. Devices attempting to access unsafe content on domains connected to COVID-19. Data from Wandera.[42]

37 Lookout, State of Mobile Phishing Spotlight, June 2020.
38 NCSC, Cyber experts step in as criminals seek to exploit Coronavirus fears, March 2020.
39 Check Point, COVID-19 Impact: Cyber Criminals Target Zoom Domains, 2020.
40 A special type of coding developed to handle non-Latin characters in domain names. It uses combinations of the letters A–Z, 0–9 and the hyphen to represent characters from sets such as Cyrillic (like Б and Д) and Kanji (like 水 and 木). This is useful because it makes the web more accessible to users around the world, but hackers have found ways to exploit it. See page 16 of the 2020 Mobile Security Index to find out more.
41 Palo Alto Networks, COVID-19: Cloud Threat Landscape, November 2020.
42 Analysis by Wandera for the MSI 2021. Based on anonymized traffic data from its user base. Baseline week of 13 January, 2020.

QRiosity can be dangerous.







Despite being around for roughly 30 years, QR codes have never really taken off, but they have come into their own during the COVID-19 pandemic. Many small retailers have adopted them as a means of contactless payment; bars and restaurants have used them to give easy access to online menus; and some contact tracing apps have leveraged them to enable users to "check in" to venues. The uptake has also been helped by Apple making it easier to scan a QR code on iOS devices—the camera app now recognizes them whereas in the past a separate app was required.

According to MobileIron, 84% of users have scanned a QR code on their mobile device, including 38% who said that they scanned one within the past week.[43]

Few of these users have probably ever thought about the security implications of scanning a blob of dots, but they can be significant.

As well as directing the user to a URL, which itself may be dangerous, a QR code can:

- Add a new network to the device's list of known (and trusted) networks
- Make a payment
- Add a new contact
- Make a call, exposing the user's phone number
- Draft an email, including populating the "to" and "subject" fields
- Send the user's location to an app
- Follow a new user on social media, exposing personal information

Any of these could be exploited by a malicious actor to perpetuate an attack.

43 MobileIron, September 2020. Study of 4,408 consumers across the U.S., the U.K., Germany, the Netherlands, France and Spain.

Attack case study: Clorox

In July, Wandera's threat intelligence engine, MI:RIAM, detected a scam related to Clorox, the well-known brand of household cleaning and disinfectant products. Reports suggest that the brand saw demand in some product categories surge by 500% in 20Q1. So it wasn't a huge surprise that bad actors tried to take advantage by launching a scam site.

The illegitimate domain, adclorox.com, reached the first page of results on leading search engines. Unlike the legitimate site, which directs consumers to retailers, it offered online sales. Except of course it didn't. Its discount prices and free shipping were all just tactics to get people to part with their money. Shoppers were left out of pocket and empty handed.

It wasn't just shoppers that were innocent victims. There's absolutely nothing to even suggest that the company did anything wrong, or that any of its data or systems were compromised. But in just a few days, the scammers were able to buy a domain with SSL certification and impersonate this well-known brand, potentially causing significant damage. And Clorox was not the only brand to be attacked in this way.

Find out more.

To learn more about how attackers exploited COVID-19, read the special report from the DBIR team, Analyzing the COVID-19 data breach landscape

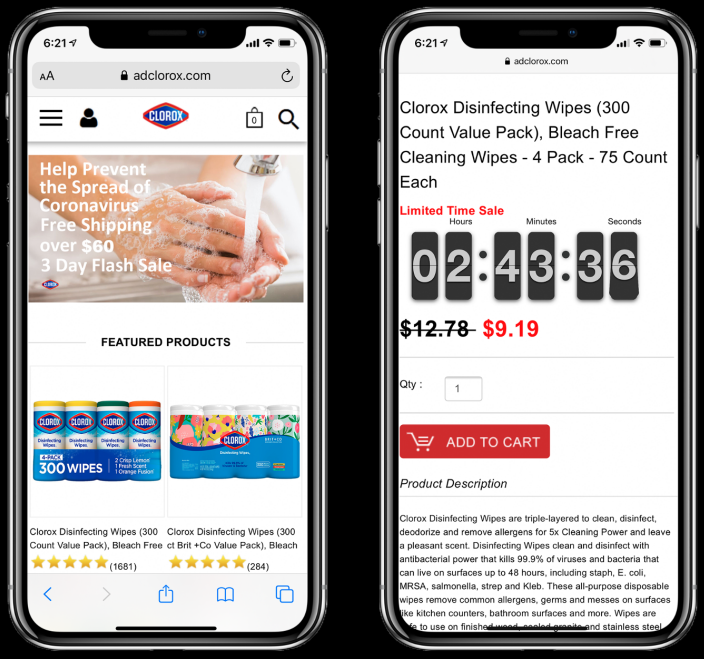


Figure 41. Actual screenshots from scam site. Supplied by Wandera.

Business email compromise

$1.14 B

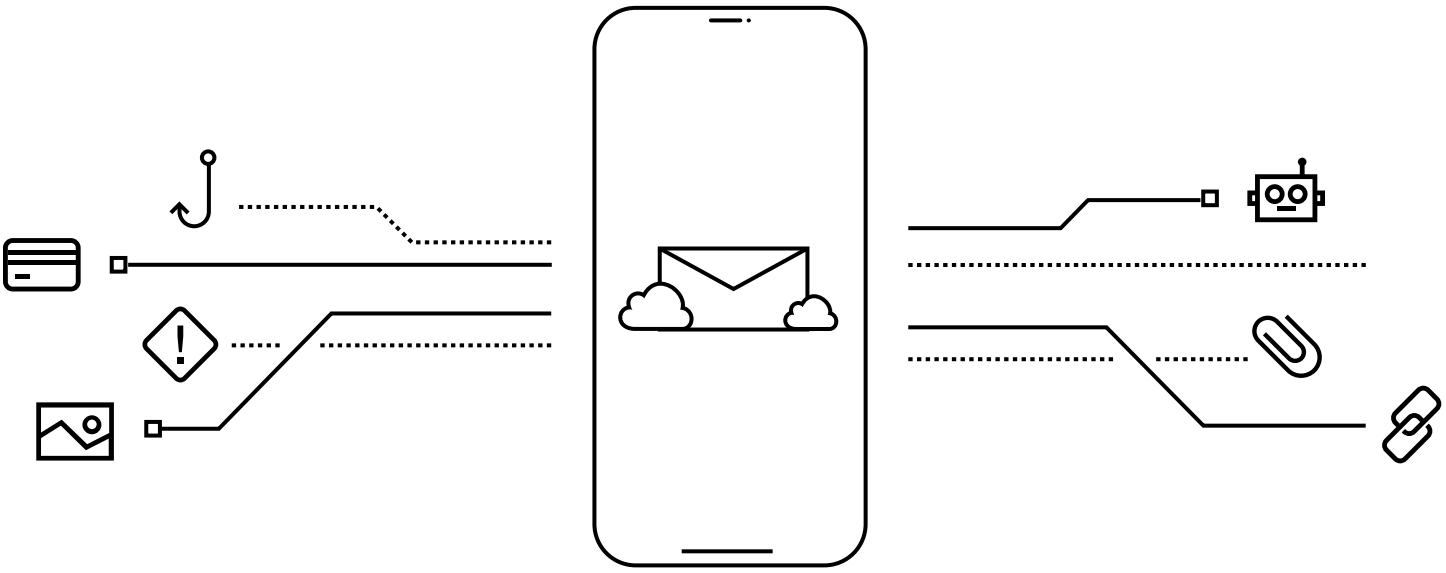
The FBI received 10,588 complaints about BECs in the first six months of 2020. The total losses encountered were $1,137,424,373.58.[44] This equates to an average loss of over $100,000. As noted in the 2020 edition of this report, the average loss from a bank robbery is about $3,000.[45]

Cloud-based applications make phishing attacks more effective and facilitate BEC attacks, which are the leading cause of financial loss in cyberattacks. The extensive control granted to users by Microsoft 365 and similar services can give attackers in possession of stolen credentials, obtained from phishing operations, a critical foothold inside the target organization. Attackers have been seen maintaining control of stolen accounts for long periods of time, eventually conducting sophisticated BEC operations using the information they receive.

Obviously it's the big-buck heists that you're most likely to hear about, but these are just the tip of the iceberg. Scams for smaller amounts—amounts that don't require multiple approvals, in a medium-to-large company—may have a better chance of success.

As awareness grows, BEC attacks are evolving. In one COVID-19-related BEC scam, the attacker used the identity of a legitimate company and advertised the fast delivery of FFP2 surgical masks and hand sanitizers. Europol said this individual had defrauded a French pharmaceutical company of 6.6 million €.[46]

Anti-phishing training for employees often relies on templates using links. But while this is a common delivery mechanism, there are others. In tests, users were more likely to fall for an attachment. And as we have reported in previous editions of this report, many phishing attacks happen outside of email, through SMS, games, collaboration tools and other apps.



44 https://www.wandera.com/analysis-covid19-internet-traffic/
45 MobileIron, September 2020. Study of 4,408 consumers across the U.S., the U.K., Germany, the Netherlands, France and Spain.
46 Europol, Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation, April 2020.

Securing against phishing

Recommendations aligned with the NIST Cybersecurity Framework

These recommendation sections are structured around the five functions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a widely recognized model based on international standards and input from public- and private-sector organizations and academia. It provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework

Identify

Identify the VAPs in your organization. Avoid the temptation to conflate VIPs and VAPs. Instinctively, you might think that Nomads like the CEO and CFO are the biggest targets, but anybody could be a VAP. Analyze what data each individual or group of individuals has access to, how they might be targeted and whether they tend to fall prey to attacks. Provide these individuals with additional awareness training. Making them aware that they are more likely to be a target could make these VAPs take more care and pay more attention to warnings.

Carry out "real-world" attack simulations that mimic the sort of interactions employees have on a regular basis with other employees, customers and suppliers.

Protect

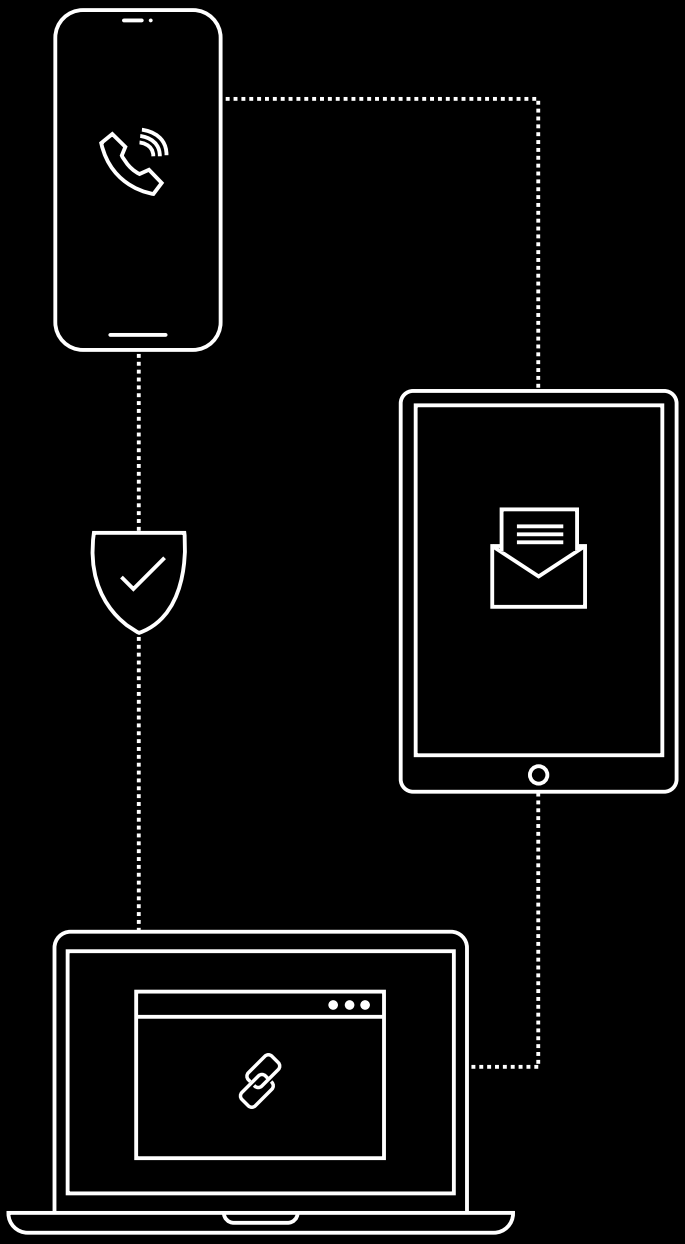
Nearly half (49%) of companies do not give employees regular training on mobile device security. Regular employee training and attack simulations can improve the chances of preventing attacks by identifying those who are especially vulnerable, including the VAPs.

Teach your employees how to spot signs of phishing—being suspicious is good. This should include checking that email addresses match who they're meant to be coming from, especially when using a mobile device. Likewise, check all URLs carefully, watching out for hyperlinks that contain misspellings of the actual domain name. It is good practice not to follow links in emails; type them out or use an existing bookmark. Similarly, be suspicious of incoming phone calls—numbers can be spoofed. It's much safer to call back on a number you know is legitimate. And, of course, it should be a rule to never supply login credentials or personally identifiable information (PII) in response to any emails or calls.

In the 2020 edition of this report, we noted that 85% of phishing attacks happen outside of email—including through SMS, apps, social media and even games. Make sure that your training and simulations aren't limited to just email.

Implement controls to verify requests for changes in account information. This could be as simple as sending a confirmation message before changes come into force. Ideally, use a secondary channel—out of band, in security speak. For example, confirm an email request with a call. But be careful, attackers can also exploit confirmation messages. Some phishing scams use messages like, "Your account details have been changed. If that wasn't you, click here."

Use a web isolation solution to restrict suspicious and unverified URLs to a protected container, like a sandbox. Also consider using this solution to isolate personal activity, like shopping and checking personal email. This can protect corporate systems and data without having to implement unpopular restrictions that users are likely to try dodging anyway.



Detect

An MTD solution can help detect and block phishing attempts however they are instigated, including via apps, social media and even QR codes—see page 54.

Help users spot malicious messages and avert attacks. Make sure the settings on their devices allow full email addresses and URLs to be viewed. One simple but effective thing you can do is configure your mail system to flag emails from outside your domain—many companies add a prefix, like [E], to the subject line. This makes it obvious when that email from the managing director is really from somebody masquerading as the boss.

Training helps, but it pays to be cynical. Attackers are constantly finding new ways to exploit human weaknesses. Implement a solution that blocks inbound email threats before they reach employees' inboxes. But assume that no matter what you do, some users will click on malicious links anyway.

Respond

Activate your standard incident response (IR) procedures. If you don't have an IR plan—51% of respondents in our survey said that their organization didn't—create one. It's vital to mitigating the damage.

Take a copy of the email (complete with headers showing routing info, etc.) and ensure that all logs are retained—this includes firewall, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and proxies. Many investigations grind to a halt due to logs having been overwritten.

Search email logs for from-address, subject line, attachment file name, etc., to identify everybody that may have received the message. Notify all users that may have been affected. Where necessary, terminate live sessions, lock accounts and force password changes.

Where possible, update your email filters to block similar messages in the future.

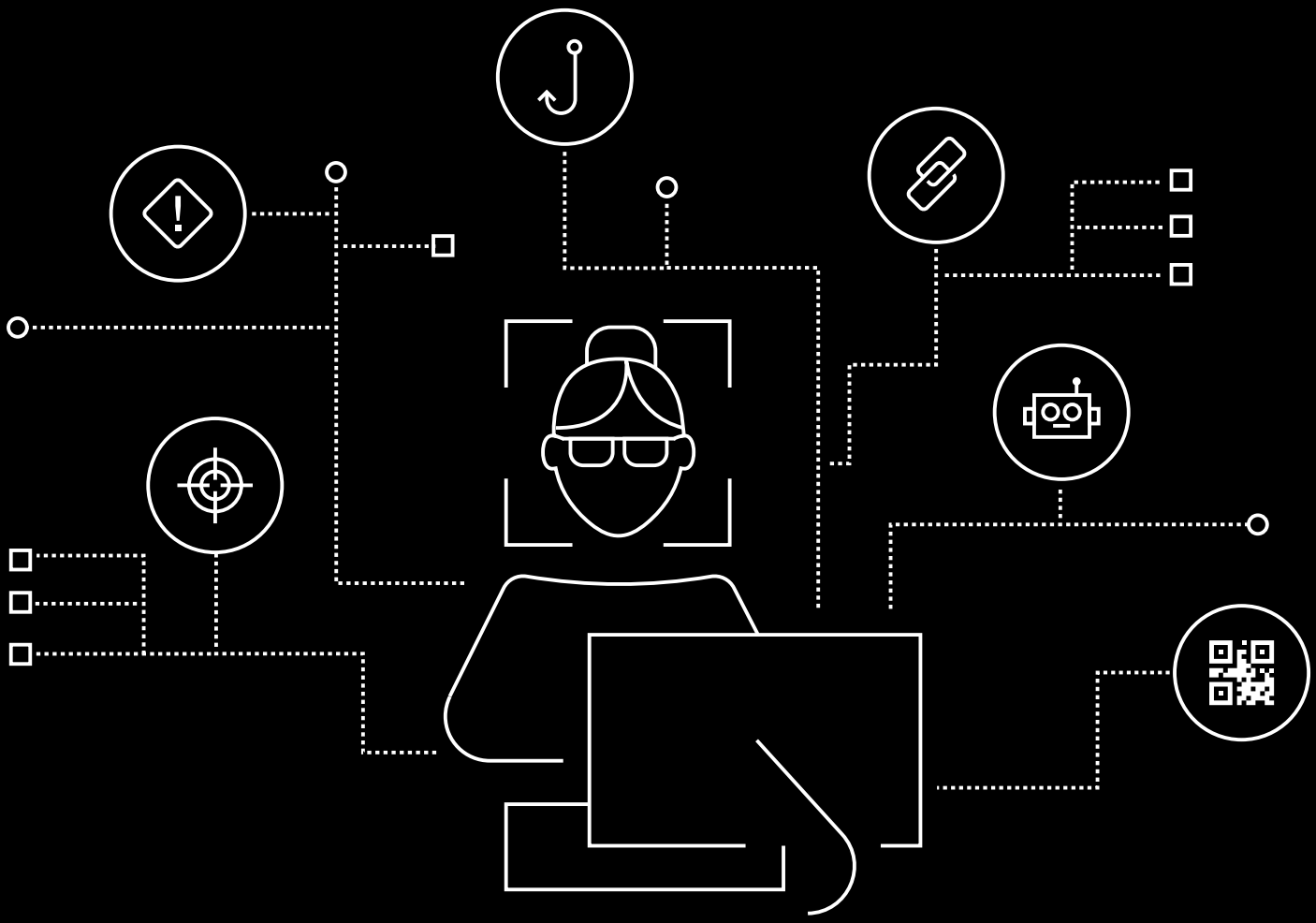
Check your threat intelligence service for similar attacks. There are also tools to search for details of threats based on hostnames, IP addresses and other details. This could give you valuable information on what damage to look for.

Recover

When discussing the historic Yalta conference, Winston Churchill is alleged to have said, “Never let a serious crisis go to waste.” Many users, even some within IT, think that a security compromise will never happen to them. Showing employees examples of actual attacks that the company has faced can help demonstrate that the danger is real.

The aftermath of a phishing attack would also be a good time to remind employees about their obligation to read and follow the company’s acceptable use policy (AUP).

MTD combined UEM can help bring devices that are out of compliance back into line through self-remediation.



Credential theft

According to Proofpoint, almost one in six (16%) people use just one or two passwords across all their accounts. A further 29% rotate between just five and 10 passwords.[47] This behavior substantially increases the likelihood of a credential stuffing attack being successful.

Many users rely on just a few passwords.

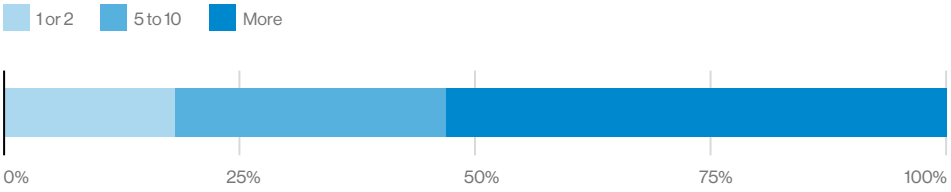


Figure 42. Number of passwords used, by number of users. Data from Proofpoint.[48]

Who said cybersecurity couldn't be fun?

This sketch is amusing but has a serious message: youtube.com/watch?v=aHaBH4LqGsI

Many companies relaxed security to enable remote working during lockdown.

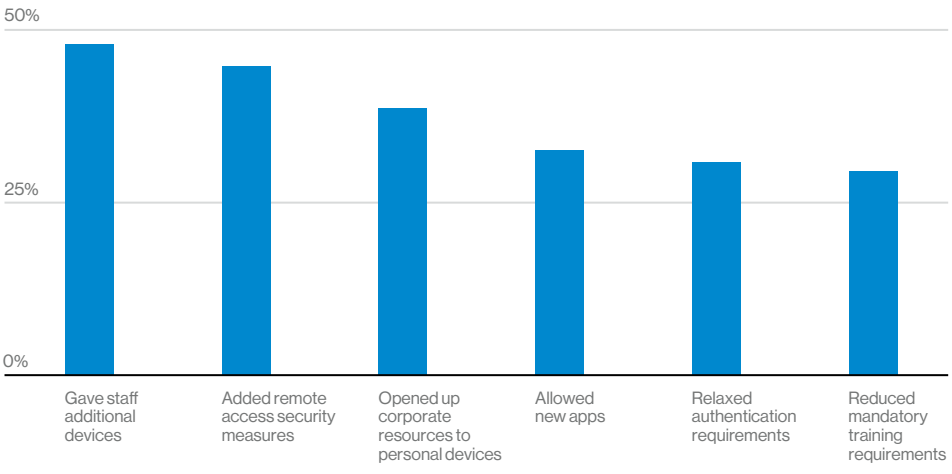


Figure 43. Which of the following measures did you take to deal with the immediate effects of increased remote working due to the COVID-19 lockdown?

1/3

Worryingly, over a third of respondents said that their company had relaxed authentication requirements to cope with COVID-19 restrictions.

47 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
48 Ibid.

Making things easier for users (and consequently support staff) is a laudable goal, but this isn't the way. Relaxing authentication requirements can make it much easier for cybercriminals to execute a successful attack. Implementing a password manager or, better yet, more sophisticated authentication would give users a better experience and maintain or even improve security. Strong authentication, of which two-factor can be part, is good. However, there's a "but." We've discussed the interception of text messages to get around authentication. There's now also malware that can be used to get the codes used for two-factor authentication. EventBot is an Android-based "infostealer" that promises to intercept SMS authentication messages from more than 200 financial applications throughout the U.S. and Europe.

Many mobile devices now incorporate fingerprint scanners. These are wonderful for productivity and user satisfaction—they are a lot less hassle than entering a complex password, especially on a virtual keyboard. But the weaknesses of fingerprint scanners are well known. It's easy to lift a fingerprint from a nice shiny screen and it's even been shown that you can capture a fingerprint from a high-resolution photograph taken from a distance. While using fingerprints for authentication is sufficient in some circumstances, it shouldn't be relied upon for anything sensitive.

Apple's Face ID is harder to fool than a fingerprint scanner or simple face recognition, but it too is fallible. However, the effort required to circumvent it makes this impractical in most situations—you probably only need to worry if you're a spy or have an evil identical twin.

Find out more.

Read more about the future of identity management and authentication on page 81.

Inappropriate use

There are many gray areas when trying to define what constitutes appropriate use, especially of mobile devices. What if employees want to use their work devices to check personal emails, stream music or scroll through social media? Many people think this is a reasonable allowance in a flexible, modern workplace. Employees often expect a bit more leeway when traveling for work—after all, they are giving up their free time and creature comforts. However, some behavior is clearly unacceptable, such as accessing adult, extreme or illegal content on company devices. This could not only harm others and damage your organization's reputation, but this type of behavior could put your company at risk. Sites of this nature are known for harboring malware and other threats.

An AUP isn't just about avoiding offending other employees, it is also about not exposing the company to greater risk.

600%

Netskope Threat Labs found a 600% increase in the number of visits to websites hosting adult content.[49]

49 Netskope, analysis based on anonymized data collected from the Netskope Security Cloud platform across millions of users from January 1, 2020, through June 30, 2020.

Most companies don't have an AUP in place.

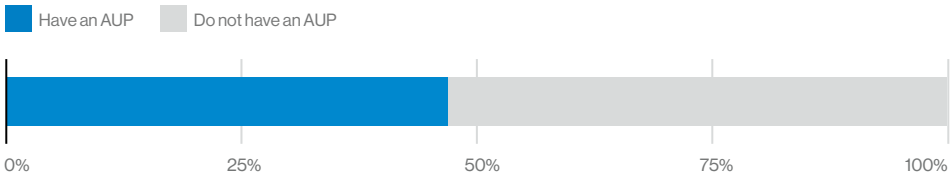


Figure 44. Which of the following do you have in place? Acceptable use policy (AUP).

Our survey found that 72% of organizations were worried about device abuse or misuse, and about one in five (19%) didn't feel prepared for it. Part of the problem is that many companies struggle to develop an effective AUP—57% didn't have one at all. Defining what counts as misuse of a work device can be an arduous task, especially if your employees need to access social media or consume a wide variety of content. But creating clear guidance, including rules for mobile-specific content, is crucial for preventing misuse.

45%

Nearly half of organizations that prohibit the use of social media are aware that employees use it anyway.

Inappropriate use remains a significant problem.

	2019		2020		Change	
	Devices	Orgs	Devices	Orgs	Devices	Orgs
Extreme	0.1%	14%	0.1%	7%	—	-7 pp
Games	47%	85%	47%	83%	—	-2 pp
Adult	21%	77%	15%	64%	-6 pp	-13 pp
Gambling	20%	75%	18%	62%	-2 pp	-13 pp

Figure 45. Inappropriate usage. Data from Wandera.[50]

Perhaps even more worrying is what's not in the policies that do exist. Key security hygiene measures are missing from many AUPs, including the use of unapproved apps (missing from 36%) and unapproved networks (missing from 41%).

It's worth noting that if there is no guidance on what is prohibited, then organizations may struggle with legal recourse. Not having these types of policies in place has led to litigation losses.

Find out more.

Our AUP tool could help you develop an effective policy for your organization.
enterprise.verizon.com/resources/reports/2021-msi-aup.pdf

50 Wandera, analysis of data from all corporate customers, January 2021.

Acceptable use and remote workers

Acceptable use becomes even more of an issue with so many more users working remotely. According to a NetMotion survey, only 36% of organizations are satisfied with their visibility into the activities of remote workers.[51]

Visibility into remote workers' activity

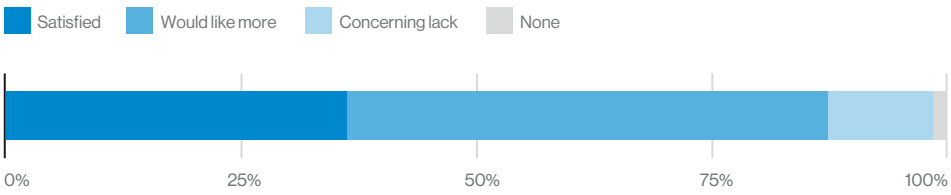


Figure 46. Satisfaction with visibility into the activity of remote workers. Data from NetMotion.[52]

That's not to say that remote workers are doing anything malicious, it's just that knowing that there's no one around can make some people less observant of the rules. This could be something as innocuous as checking their personal email or doing some online shopping. Or it could be clicking on that NSFW[53] link that they'd never open in the office.

Whenever somebody in the Commuter or Tethered categories becomes a remote worker (Omniworker or Nomad), it's vital to give them training on the risks and their responsibilities. This includes affirming that they've read, understood and will abide by the relevant policies.

File sharing

Employees often need to share files. And it's no longer just those in roles like marketing that need to share large files, like videos. We've talked about how IT professionals will sometimes sacrifice security for expediency; well, the same goes for other users. And sharing files is one way that many users have broken security policy, albeit with the best of intentions.

According to Netskope, 7% of all users uploaded sensitive corporate data to personal instances of cloud apps.[54] It's likely that the vast majority of this wasn't malicious. Some could even be unintentional, for example a user saving a file onto a personal device that they have set to sync to a service like Dropbox, Box or Egnyte. But this behavior could still lead to the exposure of sensitive data.

Many companies take measures to limit the use of removable media, like USB drives, but this is just part of the problem. Blocking file transfer sites is an option, and 31% of those in our survey do it, but is likely to only drive the problem "underground." Data loss prevention (DLP) tools can detect the exfiltration of information—whether malicious or not. It's advisable to give users an authorized—and easy-to-use—means to share files outside the company.

51 NetMotion, SDP report, June 2020. A survey of over 600 network and IT professionals across the U.S., the U.K. and Australia.
52 Ibid.
53 Not safe for work.
54 Netskope, Cloud and Threat Report, August 2020. Research was performed on anonymized usage data collected from a subset of Netskope Security Cloud platform customers (primarily North American) that had given permission for this use.

04.2 Apps

The number of apps, especially web-based apps, continues to grow apace. Malware remains a major problem, but even apps downloaded from official stores can be a threat. Apps don't even need to be malicious to pose a risk—even the clipboard could be exposing credentials.

Quick takes

- Nearly a third (31%) of companies relaxed restrictions on installing new apps to cope with lockdown restrictions
- There was a 1,200% increase in use of collaboration apps during the first 90 days of lockdown
- The number of cloud apps in use continues to grow, with the largest enterprises now using more than 7,000
- Analysis of mobile apps found that 4% leak credentials[55]

55 Wandera, analysis of mobile apps in 2018.

Trends in app use

Nearly a third (31%) of companies relaxed restrictions on installing new apps to cope with lockdown restrictions. This varied quite significantly between industries: Just one in five (21%) manufacturing companies relaxed restrictions, whereas nearly half (47%) of media companies did. Media companies were also much more likely to enable employees to work from home.

Growth in use of collaboration apps

COVID-19 has had a major impact on the types of apps used by companies. Verizon network data for the first 90 days after lockdown showed a 1,200% increase in data use via collaboration tools. This was a result of both more users and greater use per employee.

80%

With the growth in remote work came an 80% increase in the use of collaboration apps as remote workers sought to remain connected with their colleagues.[56]

According to Netskope, the number of employees using collaboration apps increased by 20%. The types of collaboration apps that saw the greatest increase included:

- Chat applications (such as Slack and Google Chat)
- Video conferencing apps (such as BlueJeans, Cisco Webex, Microsoft Teams and Zoom)
- Specialty apps (such as Miro, an online whiteboard tool)[57]

Manufacturers were least likely to relax restrictions on new apps.

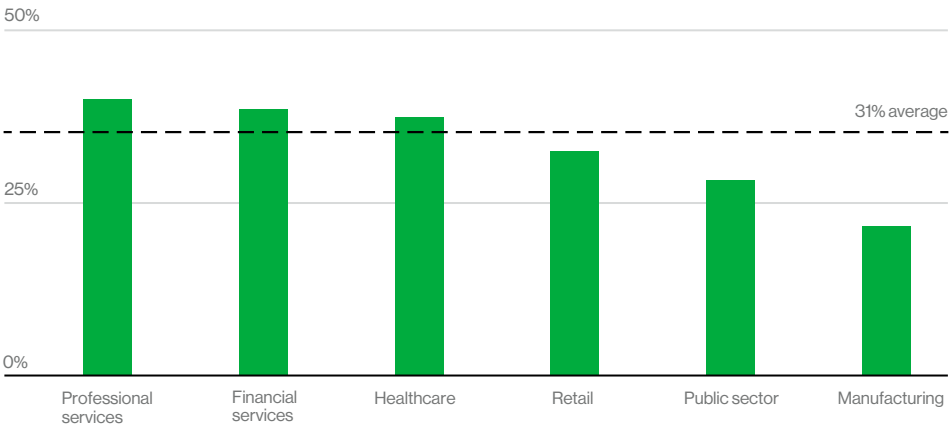


Figure 47. Which of the following measures did you take to deal with the immediate effects of increased remote working due to the COVID-19 lockdown? Allowed installation of new apps. [n=598]

Network traffic growth during first 90 days after lockdown, by app type

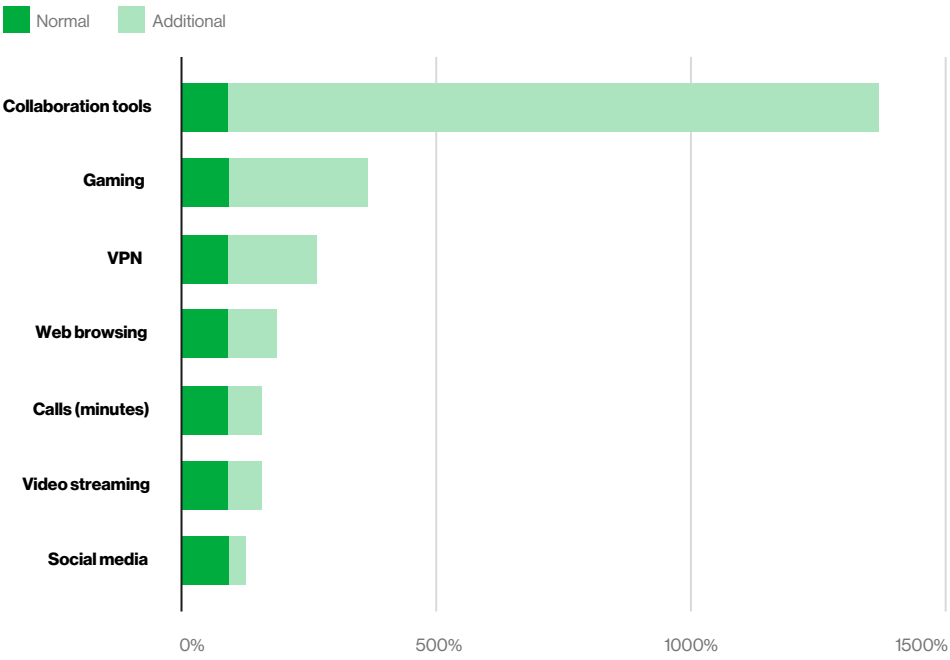


Figure 48. Based on Verizon network data from the first 90 days following lockdown.

56 Netskope, Cloud and Threat Report, August 2020. Research was performed on anonymized usage data collected from a subset of Netskope Security Cloud platform customers (primarily North American) that had given permission for this use.

57 Ibid.

App permissions

There are literally millions of apps available. While there's a "long tail,"[58] there are nearly 120,000 apps with more than 500,000 installs in the Google Play Store alone. Analysis carried out by Wandera for this report found 96,715 apps in use on enterprise Android devices and 109,887 on enterprise iOS devices. The vast, vast majority of these were on fewer than 1% of devices. This shows the enormous diversity of apps in use, and consequently the scale of the problem of managing what apps are installed and the permissions given to them.

Many of these apps will be well coded and respect personal data and thus present little risk. But even these "harmless" apps can be compromised and pass personal or corporate data to unscrupulous third parties. This shows why an MTD solution is so important to mitigating the risk. As well as blocking known threats and spotting anomalous behavior, MTD can help manage what permissions apps are granted.

Android: 99.4% of the 96,715 Android apps seen on enterprise devices were installed on fewer than 1% of devices.

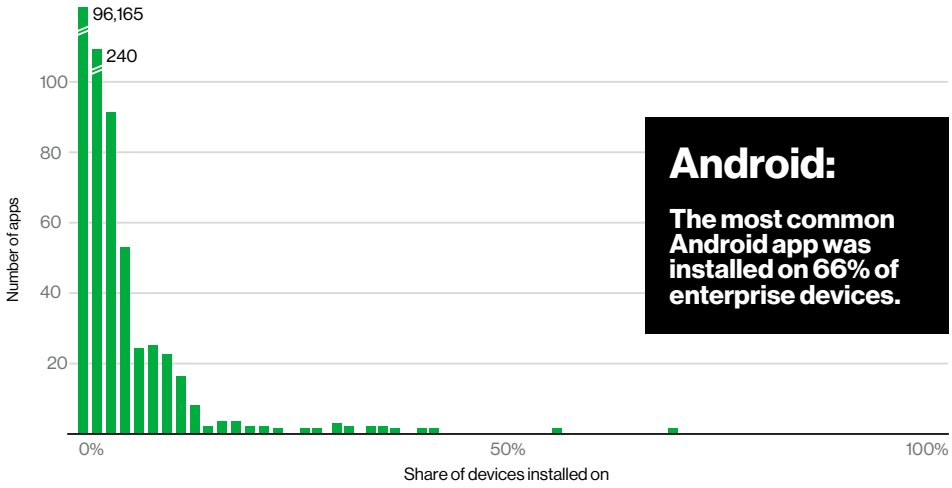


Figure 49. Number of Android apps by percentage of devices installed on. Data from Wandera.[59]

iOS: 99.8% of the 109,887 iOS apps seen on enterprise devices were installed on fewer than 1% of devices.

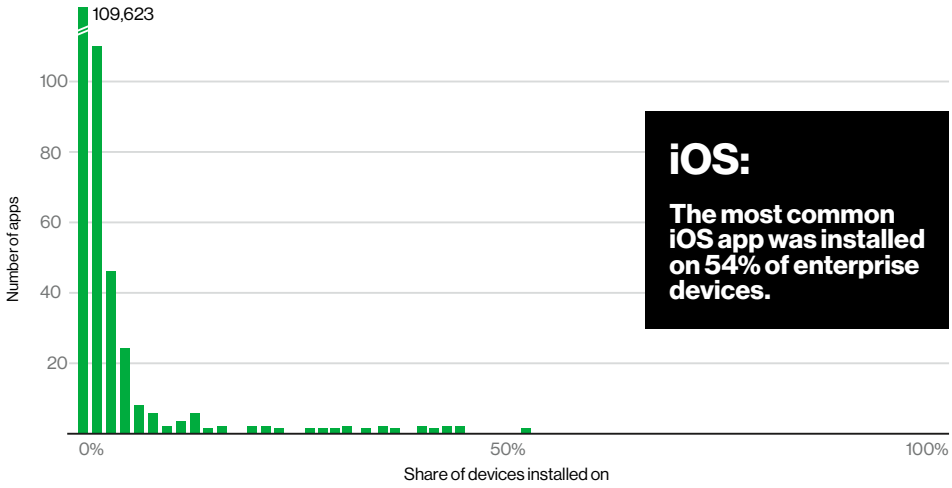


Figure 50. Number of iOS apps by percentage of devices installed on. Data from Wandera.[60]

58 The term "long tail" was coined by Chris Anderson in 2004. It refers to the distribution of sales of a large catalog of products. Typically, most sales will be for a small number of products, with purchases quickly "tailing off." It is a similar concept to the "Pareto principle" or "80:20 rule."

59 Wandera, analysis based on aggregated data from customer base in January 2021.

60 Ibid.

Social media and weather apps requested the most permissions.

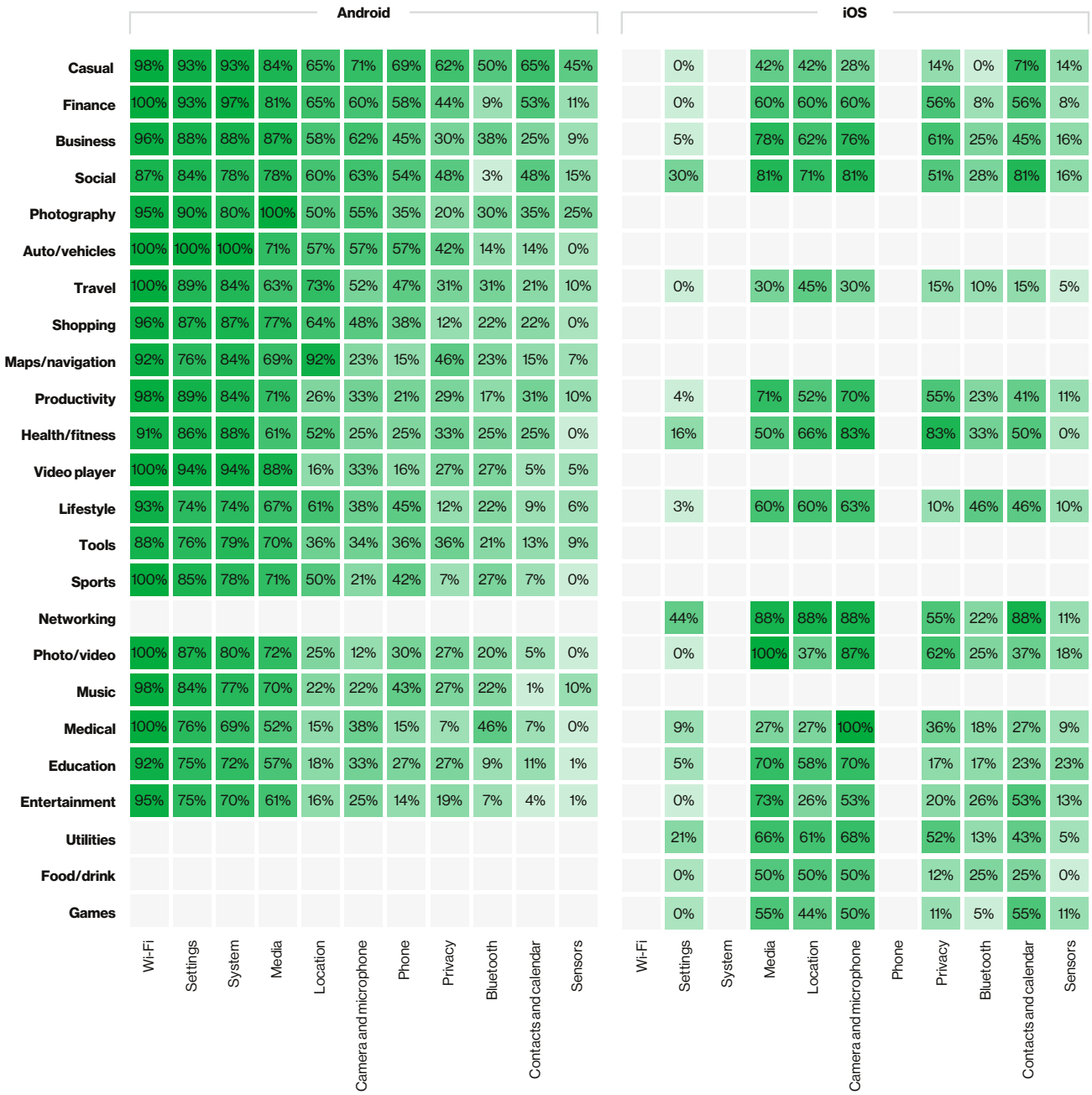


Figure 51. Proportion of apps per app category declaring said permission. Only top 10 permissions listed. Data from Wandera.[61]

Some apps collect data without explicitly asking for permission.

Some apps collect data without explicitly asking for permission. Others completely ignore users' preferences. Wandera Threat Research Labs helped the Wall Street Journal investigate "Weather Forecast—World Weather Accurate Radar," a weather app with over 10 million downloads from the Google Play Store. The investigation was prompted when users spotted that the app was requesting unusual amounts of information, despite not having obtained permission to do so. Wandera found that the app was siphoning off user data, including detailed geographic location, email addresses and device unique identifiers. Even when the app did ask for permission, this didn't affect its behavior. The privacy prompt was essentially a gimmick to lull users into a false sense of security.

61 Wandera, analysis in January 2021.

Password snooping

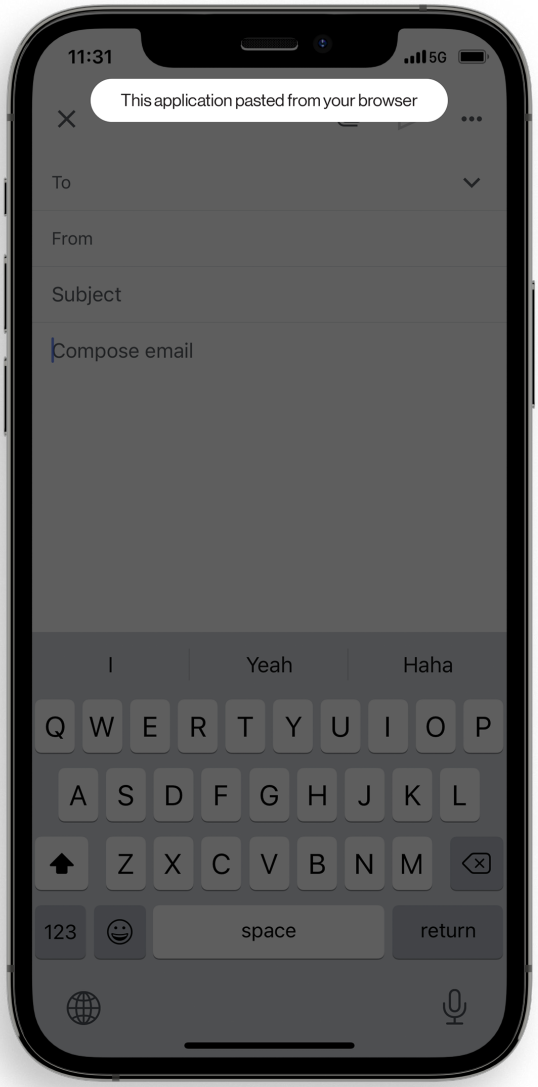
In 2020, LinkedIn and other iOS apps were found to be capturing the contents of the clipboard after every keypress. Many other apps were doing it on open. There are legitimate reasons for doing this, like some smart login methods (see below), and LinkedIn blamed the practice on a bug. But this could easily be exploited to capture passwords.

The concern isn't just that apps are doing this, but also that they are able to. iOS 14 introduced a new feature that informs you when an app accesses the clipboard, but this is like closing the stable door after the horse has bolted.

This vulnerability is even more of a concern because Apple devices have a feature called handoff. This allows you to copy something on your Mac and paste it on your iPhone. Using a password manager that auto-fills passwords without using the clipboard could help mitigate the risk of this vulnerability.

Smart login

Some apps implement social sign-in (like "Sign in with Google") by opening a web page, prompting you to authenticate and then, if successful, opening the app. If opening the app fails, some apps, including Slack, prompt the user to copy a sign-in key from the web page—some even do it automatically. Then when you open the app, it reads the clipboard and logs you in automatically.



62 Wall Street Journal, Popular Weather App Collects Too Much User Data, Security Experts Say, January 2019.

Leaky apps

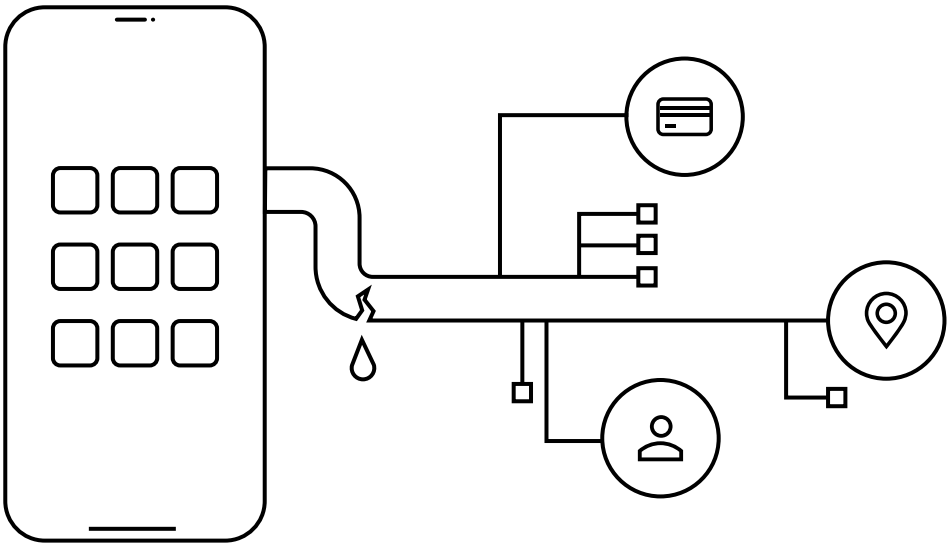
One in 25 (4%) apps leak sensitive credentials.[63] That might not seem like a lot, but it only takes one to compromise a user's authentication details. Sometimes this isn't malicious; it can be the result of bad coding or using insecure services to transmit and store app data.

Common types of data that's leaked include:

- Email address
- User ID
- Password
- Credit card data
- Location

And, as we discussed earlier, users often use very few unique passwords, so the exposure of one set of credentials could lead to the security of many apps, web apps, email accounts and other systems being compromised.

Something like location may not seem like particularly sensitive data, but it can give away a user's hobbies, sexual orientation, political affiliation and more. This information could be used for extortion, to craft more targeted phishing messages or even identify opportunities for real-world crimes.



Virtual leaks, real-world crimes

Wandera has identified numerous instances of vehicle tracking systems with serious security weaknesses. This includes failing to protect data, including login information and location data, during transmission to a back-end service provider. This may seem trivial, but consider these scenarios:

Knowing the precise location of a truck carrying spent nuclear material or a vehicle carrying a senior government figure or dignitary could be of enormous value to a terrorist organization.

Vehicle tracking technology isn't just used on 18-wheelers and courier bikes. Many high-end supercars—and even F1 and NASCAR racers—are fitted with sophisticated user interfaces and security systems that use mobile connectivity. Being able to locate and track these vehicles could, of course, be of great interest to a thief.

Tracking the movements of an organization's vehicles could expose details of its supply chain, customers and other sensitive information.

63 Wandera, analysis of mobile apps in 2018.

Malware

Nearly 30% of U.S. workers said that they thought that malware is a type of hardware that boosts a Wi-Fi signal.[64] That could just be a warped sense of humor, but it seems unlikely that people would make the effort to fill out the rest of the survey professionally and suddenly get witty on this one question. This serves as an important reminder that what might seem obvious to those working in IT and well-read on cybersecurity may be a mystery to many others. There's still a lot to do in educating people about the threats and how to counter them—both in their personal lives and as employees, business owners or government officials.

The prevalence of mobile malware fell in 2020, but overall the trend is still upwards.

Fewer users encountered mobile malware.

	2018	2019	2020	CAGR
Organizations	2.1%	10.1%	8.2%	+198%
Devices	0.03%	0.33%	0.17%	+238%

Figure 52. Incidence of mobile malware. Data from Wandera.[65]

New methods

We talked about mal-innovation in malware in the previous edition of this report. This inventiveness continued in 2020. This included clever techniques, like malicious functions that remain dormant until triggered to avoid detection. This technique has been used to bypass controls and get malicious apps into official stores.

Restricting users to apps from official app stores is far from watertight, but it can make a helpful contribution to reducing the risk of a malware infection. Despite this, many companies have quite liberal policies on the installation of apps.

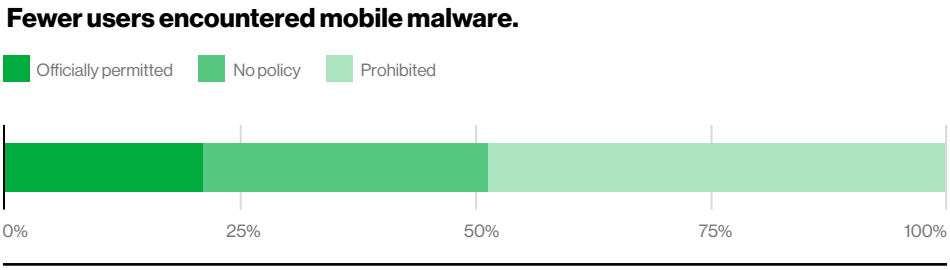


Figure 53. What is your policy for each of the following on company-owned/controlled devices? Apps not from company or official app store. [n=598]

In mid-2020, Check Point identified a substantial increase in the number of malicious applications in the official Google Play store. This included applications infected with the Tekya clicker, BearCloud and Haken. And indeed, when researchers examined 150,000 Android apps, they found that almost 7% of the apps in the Google Play store contained hidden backdoors.[66]

One of the most innovative techniques that we saw in 2020 was an attack where the threat actors used an international corporation's own MDM system to distribute malware to more than 75% of its managed mobile devices.[67] This shows that an MDM is not sufficient to secure mobile devices and makes the case for effective MTD.

64 Proofpoint, State of the Phish, August 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
65 Wandera, analysis carried out in January 2020. Data from enterprise user base.
66 Check Point, Cyber Attack Trends: 2020 Mid-year Report, July 2020.
67 Check Point, First seen in the wild—Malware uses Corporate MDM as attack vector, April 2020.

Malware as a Service

Attackers don't need to be as innovative or technically savvy as those mentioned earlier.

Like the ransomware kits that we featured in the 2018 edition of this report, there are easy-to-use kits that make it easy to create criminal malware campaigns even if you don't have much technical knowledge. That's not to say that a bored teenager or disgruntled former employee is the greatest threat. These tools could equally be used by more organized attackers to mount more effective attacks and more of them.

One of the most-often encountered remote access Trojans (RATs) is Agent Tesla. It dates back to 2014, but its functionality has increased every year. It can monitor keyboard activity, take screenshots, access the clipboard and more. Agent Tesla has been observed stealing credentials from a number of common applications, including Google Chrome, Mozilla Firefox and Microsoft Outlook email client. In 2020, the ability to extract Wi-Fi profiles was added.

Unlike some other cybercriminal tools, you don't even have to venture into the recesses of the dark web to get hold of Agent Tesla. It's promoted and sold just like a legitimate app. There's also an as-a-Service option with several tiers ranging from $15 to $69—higher tiers even come with 24/7 support!

Ransomware

Ransomware continues to cause problems for organizations worldwide. Public sector organizations seem to be particularly prone to these attacks, but that might just be because they tend to be subject to tougher disclosure rules. After attacks peaked a few years ago, many organizations put measures in place to thwart this sort of attack. "White hat" hackers have also published tools to decrypt computers affected by attacks using common ransomware kits and variants.

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

—Donna Gregory, Unit Chief, FBI Cyber Division[68]

Faced with better-prepared victims, attacks have evolved their techniques. Instead of simply locking the files on the infected device, newer variants target files you have stored in online services like Google Drive and Microsoft 365. An even more alarming variation is doxware (or leakware), which as well as encrypting your personal files threatens to publish them online.

Ransomware as a service is a lucrative business.

GandCrab, one of the most infamous ransomware-as-a-service (RaaS) operations, announced its "retirement" in 2019. It claimed to have amassed $2 billion through selling its customized malware. In 2020, Maze, another well-known RaaS provider, announced that it was closing down after netting millions from both public- and private-sector organizations. Not paying the ransom can be expensive too. One IT services company that was hit by a Maze attack in April 2020 has estimated the clean-up costs at $50 million to $70 million.[69]

68 Donna Gregory, Unit Chief, FBI Cyber Division, 2020.
69 Techcrunch, Cognizant confirms Maze ransomware attack, says customers face disruption, April 2020.

Attack case study: Lucy ransomware[70]

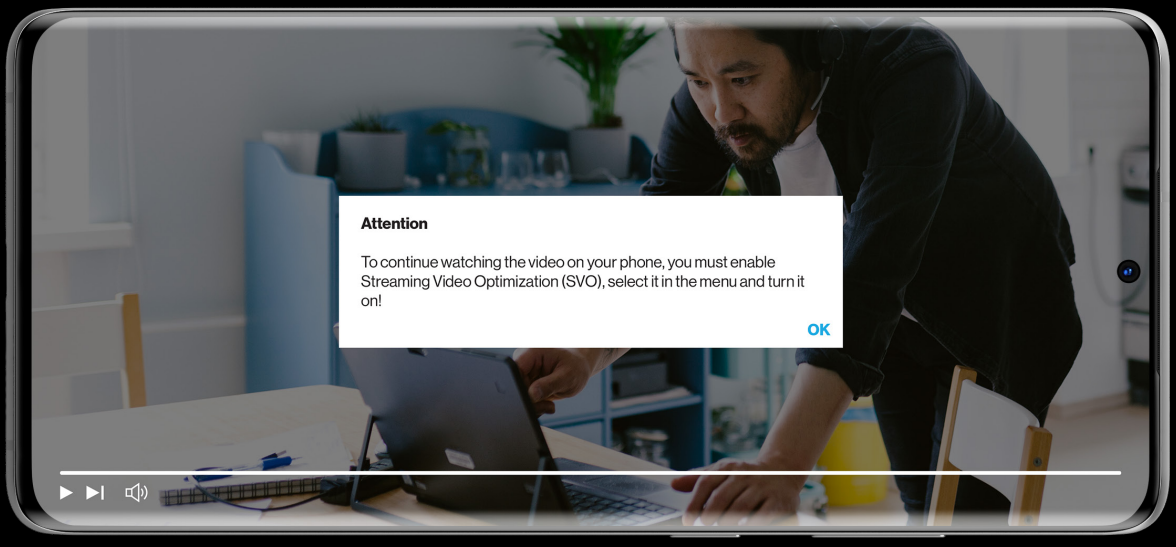
Ransomware attacks have been a part of the security landscape for a long time. We are familiar with infamous malware such as CryptoLocker, WannaCry and Ryuk, which have caused enormous damage to organizations around the world. Ransomware targeting phones and tablets has been around since at least 2014, but has been much rarer. This is likely largely due to so little data being stored on these devices; a wipe and reinstall is a much less disruptive solution to an attack than it would be on a laptop. But with other options running out, as defenses improve, attackers are finding ways to create disruptive mobile ransomware attacks.

An example is the "Black Rose Lucy" malware family, originally discovered in September 2018. It is a Malware-as-a-Service botnet and dropper for Android devices. It reemerged in 2020 with new ransomware capabilities that allow it to take control of victims' devices to make various changes and install new malicious applications. Check Point researchers have discovered more than 80 examples of this variant in the wild, mainly distributed via social media and IM apps.

When downloaded, Lucy encrypts files on the infected device and displays a ransom note, purporting to be from the FBI, that accuses the victim of having pornographic content on their device. The message states that, as well as the device being locked, the user's details have been uploaded to the FBI Cyber Crime Department's Data Center and lists a string of legal offenses that the user is guilty of. The victim is then instructed to pay a $500 fine to avoid further action and unlock their device.

What's particularly clever about Lucy is how it gets around protections added to the Android OS to prevent attacks. The OS only requires users to manually configure applications to give them device administrator privileges. This involves explicitly giving consent in a pop-up window or navigating through a series of system settings.

Lucy takes advantage of the Android accessibility service, which mimics a user's screen clicks and has the ability to automate user interactions with the device. It displays a message asking the user to enable "streaming video optimization." Hey, smoother Netflix, what's not to love? By clicking OK, the user is actually granting the malware the permission to use the accessibility service and hence admin privileges.



70 Check Point, Lucy's Back: Ransomware Goes Mobile, April 2020.

Securing against malware

Recommendations aligned with the NIST Cybersecurity Framework

These recommendation sections are structured around the five functions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a widely recognized model based on international standards and input from public- and private-sector organizations and academia. It provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework

Identify

Audit company systems and processes for vulnerabilities to malware.

Actively monitor mobile devices for known malware and permission abuse.

Develop anti-malware policies and implement them across all networks and devices.

Subscribe to a threat intelligence service to stay abreast of the latest malware threats.

Conduct regular network penetration tests to identify possible vulnerabilities. Make sure that the results are thoroughly analyzed and remedial action carried out.

Protect

Make sure that your cybersecurity training programs cover preventing malware infections. This should include guidance on spotting dangerous links, identifying suspicious attachments and how to use removable media (like USB drives) safely.

Deploy anti-malware functionality to all devices. This may be included within your antivirus or endpoint protection solution.

Add content filtering to all external gateways to make it more difficult for attackers to deliver malicious content to users via their web browser and email.

Where possible, prevent the use of removable media such as USB drives and memory cards. At the very least, educate users on the dangers of using untrusted devices, disable auto-run functions and set up devices to automatically scan removable media for malicious content.

If you suffer a ransomware infection, backups may be the best way to recover your critical data. But just installing a backup solution isn't enough. Ensure that backups are not connected to the computers and networks they are backing up – for example, physically store them offline. It's also crucial to verify backups. A real-life emergency, when you need to restore data, is a bad time to find out that there's a problem. Because it's end users who are targeted, it's important to make employees aware of the threat of ransomware.

Consider implementing controls to prevent the execution of programs in locations commonly used by ransomware, such as temporary folders used by browsers and compression/decompression applications.

Use deny listing on external gateways to block access to known malicious websites.

Detect

Implement an MTD solution to quickly identify potential threats.

Educate users on how to identify and report suspicious or unexpected system behavior. Something a user may just see as an annoyance–like a device constantly needing charging – could be an indicator of a malware compromise.

Monitor devices for unusual behavior – including excessive data transfer and out-of-hours use – that could indicate that an application has been compromised.

Respond

Identify all infected devices and physically disconnect them from the network.

Suspend the login credentials of any accounts that may have been compromised.

Notify all users of the compromised app and what action to take. Deleting the app may not always be the best course of action, as this could destroy important forensic data.

Recover

Reset all credentials, especially those with administrator privileges, that may have been compromised.

Wipe all infected devices and reinstall from the OS up.

Conduct a post-mortem exercise to determine how the malware managed to get through and where controls, processes and technology fell short. Create and distribute an "after-action" report.

04.3 Devices and things

With the volume of devices a modern enterprise relies on, keeping them all up to date can seem like a Sisyphean[71] task. With more and more devices, the danger of lost or missing devices grows. But it's not just the quantity of devices that's growing, the variety is growing too. Today there are smartphones, laptops, tablets, hybrids (like Microsoft Surface), Chromebooks, wearables and a seemingly endless range of IoT devices.

Quick takes

- Seventy-one percent of U.S. workers have allowed friends or family to use their work devices[72]
- Over half (56%) of respondents said that they were worried about device loss/theft
- Thiry percent of IoT respondents said that these devices are of less interest to hackers than other systems
- The vast majority (91%) of IoT respondents said that they are collecting PII, and 22% of those weren't encrypting it

71 In Greek mythology, Sisyphus, a king of Corinth, angered the gods by cheating death. As a consequence, Zeus sentenced him to roll a huge boulder up a hill in the depths of Hades forever. Sounds a lot like the ancient equivalent of patching devices.

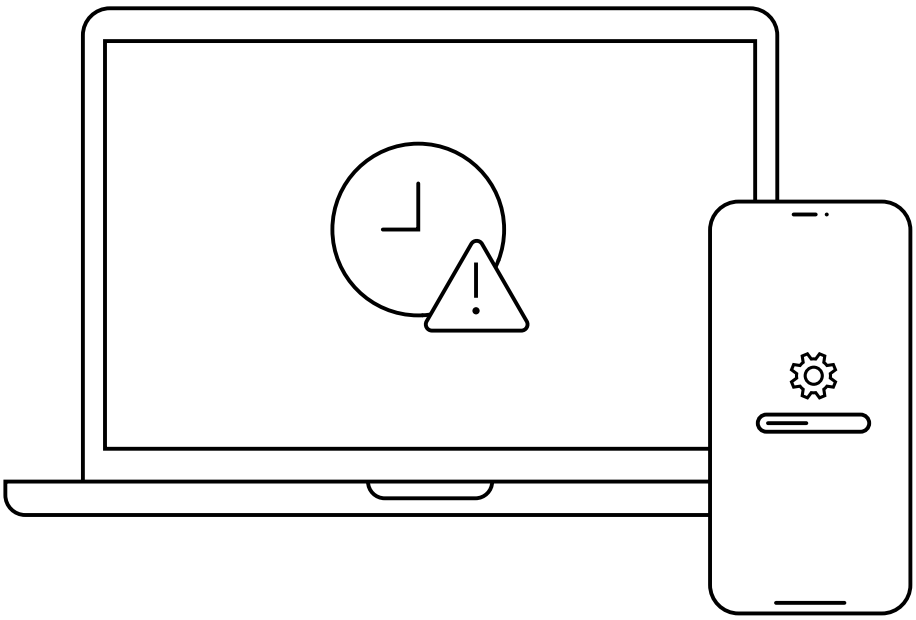
72 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.

Out-of-date operating systems

A notification to update your device OS is about as welcoming as an early morning alarm call. It's little wonder that so many of us hit the "snooze" button.

Often, the hassle doesn't seem worth it. In between the major OS updates with the cool new features, there are often numerous minor updates with little obvious benefit to the user. But these updates normally include all kinds of important security patches. Missing an update, even a minor one, can make a device more prone to compromise—putting data and systems at risk.

In previous years, we've looked at the state of OS updates by analyzing minor updates, like 13.1 to 13.2. Even these "minor" updates can contain important security updates and shouldn't be ignored. But this time we've focused on the two major updates in 2020: Android 11 on September 8 and iOS 14 on September 16. Close to four months after the updates, the number of devices—especially Android devices—that were running an out-of-date OS was extremely high.



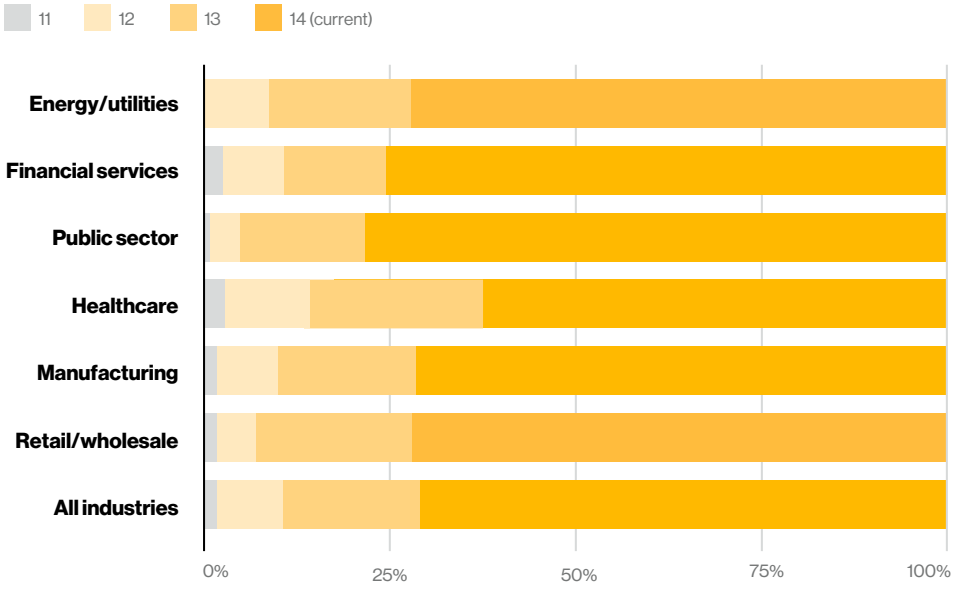
There are several factors driving the lag between OS updates being released and users installing them:

Device replacement cycles are lengthening. After years of rapid innovation, the pace of change slowed. Recently, most hardware updates have revolved around increasing battery life and further improvements to the camera. With fewer "must-have" advancements, many owners have chosen to hold on to their devices longer. The release of 5G devices should reverse that trend—at least for a while.

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

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

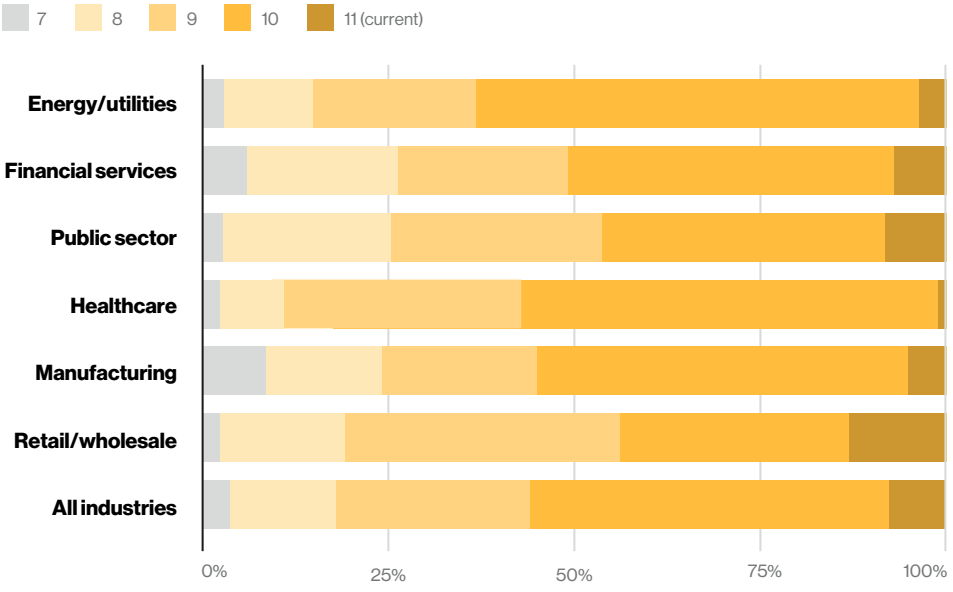
Many iOS devices were running an out-of-date OS.



Nearly three out of every 10 iOS devices were running an out-of-date version of the OS.

Figure 54. Mobile device OS version by industry (iOS devices). iOS 14 was released September 16, 2020. Data from Lookout as of January 6, 2021.[73]

But the picture was far worse for Android devices.



More than nine out of every 10 Android devices were running an out-of-date version of the OS.

Figure 55. Mobile device OS version by industry (Android devices). Android 11 was released on September 8, 2020. Data from Lookout as of January 6, 2021.[74]

73 Lookout, based on analysis of all active iOS devices, January 6, 2021.
74 Lookout, based on analysis of all active Android devices, January 6, 2021.

Lost or stolen devices

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

Over half (56%) of respondents said that loss/theft isn't a threat that they are worried about—and that's not just because nobody went anywhere in 2020. We've seen similar numbers in our previous surveys.

One of the reasons why so few organizations are worried is because loss/theft is one of the types of compromises that's easiest to mitigate. Protections like device encryption and remote wipe are now standard with most types of user devices and MDM. But that doesn't mean that people are using them.

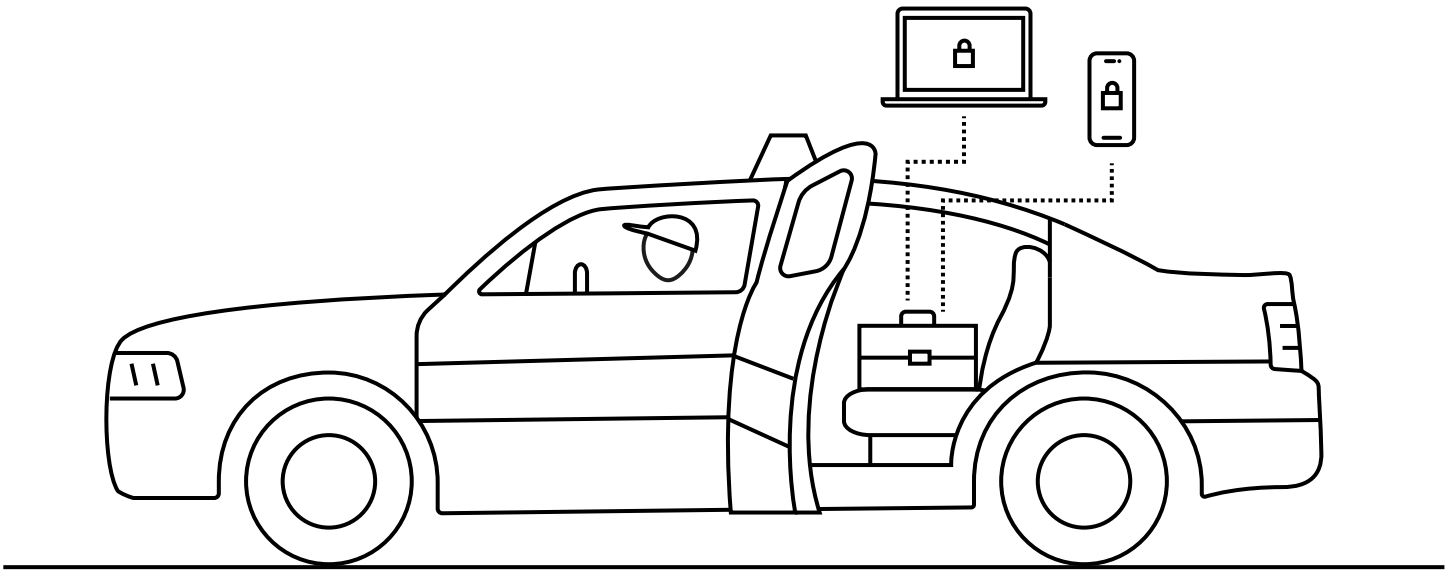
Whole-disk encryption and PIN security codes should be activated as a standard precaution on all devices. With these simple precautions in place, even if a device is stolen, the data it holds will be—for all intents and purposes—worthless to the attacker. Under many mandatory disclosure rules, you may not even need to notify regulatory bodies about lost or stolen devices if they are encrypted.

37%

Only 37% of companies in a VMware customer survey said they were using whole-disk encryption on laptops.[75]

3%

In almost a third (30%) of organizations, at least one user had a device with the lock-screen feature disabled—3% of devices overall.[76]



75 VMware customer research, 2019.
76 Wandera, analysis of global customer base between January 1, 2020, and December 31, 2020.

U.S. employees were most likely to let others use their work device.

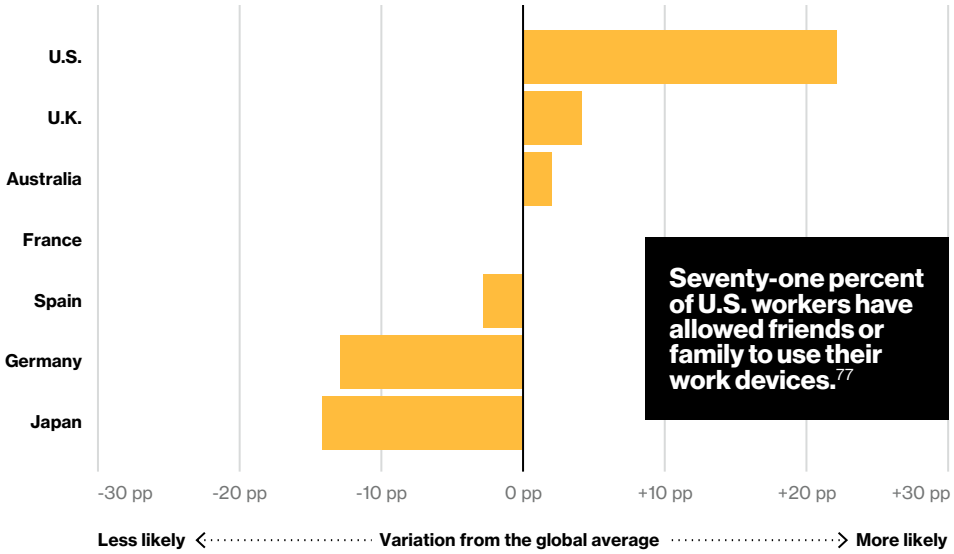


Figure 56. Share of users that let friends or family members use a work device by country, variation from the global average. Data from Proofpoint.[78]

And it wasn't even just for urgent tasks. Checking personal email and social media were the two most common reasons for letting others loose on company devices.

Many employees let friends or family use their work devices.

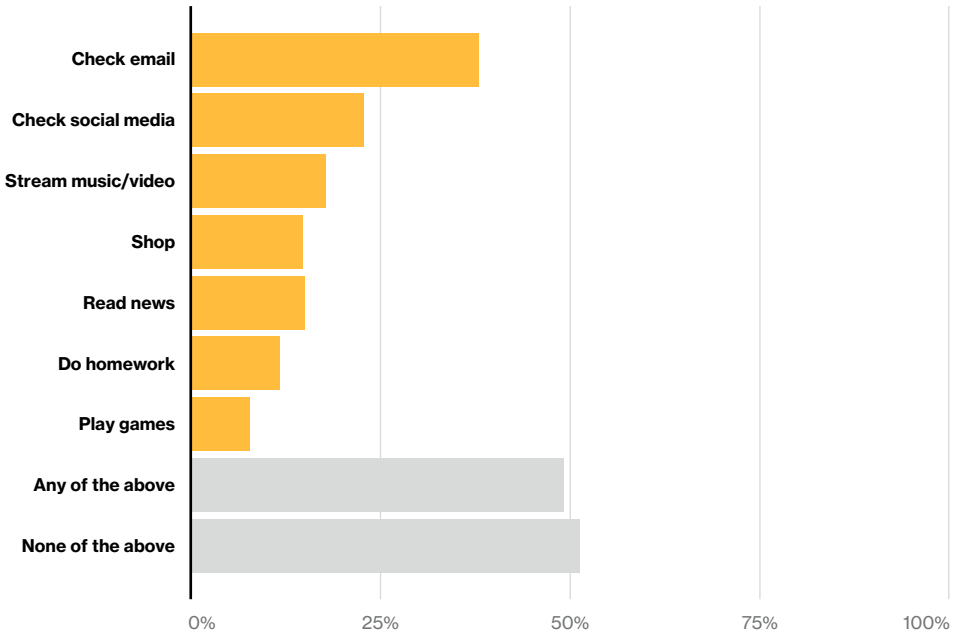
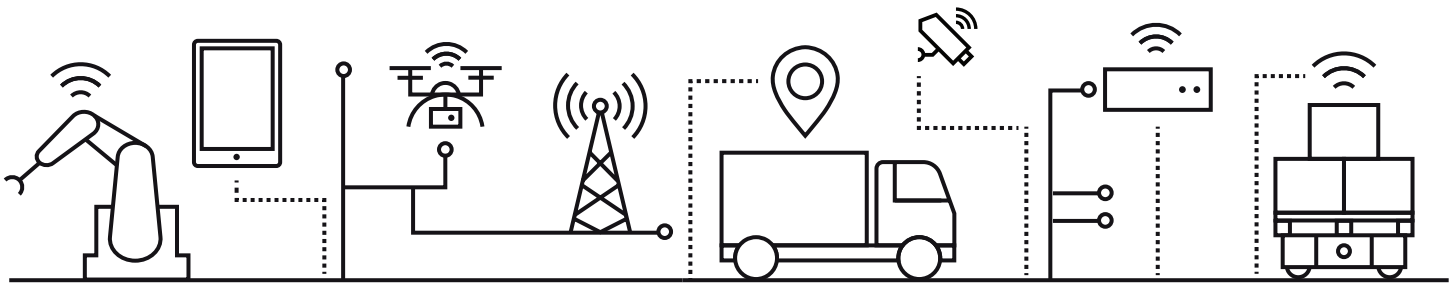


Figure 57. Why users let friends or family members use a work device. Data from Proofpoint.[79]

77 Proofpoint, State of the Phish, August 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
78 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
79 Ibid.

IoT devices



Respondents to the IoT track of our survey were slightly more likely to admit to having suffered a compromise involving a mobile or IoT device—26% versus 22% for mobile respondents.

Worryingly, the share of IoT respondents that think these devices are of less interest to hackers than other systems grew from 26% in our previous survey to 30% this time around.

Stories about connected cars being susceptible to hacking seem to have fallen off the radar. The truth is, while this made for appealing headlines for journalists and bloggers, the biggest risks were actually much more mundane.

The interception and modification of IoT while in transit can have serious consequences, especially in industrial or manufacturing environments. For example, inaccurate or falsified data transmitted from heat or temperature sensors could not only ruin batch production, it could destroy equipment or endanger employee safety. Many hackers are also using malware to turn IoT devices into a botnet—an army of devices typically used for malicious purposes, like distributed denial of service (DDoS) attacks. And, of course, a single compromised IoT device could offer hackers a virtual open door to your network and everything that's attached to it. A well-known example involved a hacker getting into an HVAC maintenance company and using its access to customer systems as a stepping stone to steal the details of millions of payment cards from a major retailer.

Securing IoT devices presents distinct challenges compared to other mobile devices. These fall into three broad areas:

1. Variety

The sheer volume and diversity of IoT devices can present enormous logistical obstacles to effective device security. One in five (20%) of our IoT respondents said that they had 1,000 or more devices in operation; 10% had more than 5,000. It doesn't help that many IoT products have been found to have extremely weak cybersecurity—including security devices such as smart locks, doorbells and, ironically, security cameras.

2. Distance

Many IoT devices are out in the field. This can make them vulnerable to physical tampering or network attack and harder to update or replace. Just 12% of IoT respondents said that none of their IoT devices are difficult to access—for example, embedded in a system or in a remote location.

Isolation can also make devices vulnerable to SIM theft, one of the simplest types of attack to carry out—often all that's required is a screwdriver. All the hacker has to do is break open the connected device, such as a smart lamppost, and remove the SIM. This can then be put into another device, giving the user free calls and data at the organization's expense. Only 7% of mobile respondents said that they were concerned about SIM theft, but this leapt to 23% among IoT respondents.

3. Longevity

Over half (54%) said that some of their IoT devices had an anticipated lifetime of five years or more—up from 36% in our previous report. This would be very old for a smartphone or laptop. Combined with the difficulty of updating devices, this can make it hard to keep IoT protected against constantly evolving threats.

Securing IoT devices

Recommendations aligned with the NIST Cybersecurity Framework

These recommendation sections are structured around the five functions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a widely recognized model based on international standards and input from public- and private- sector organizations and academia. It provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework

Identify

Thoroughly review the security before you purchase anything. Whether you are buying off-the-shelf solutions or components to build your own IoT devices, ask potential vendors to supply details of the security measures they take, and review them for robustness. Pay particular attention to their authentication, encryption and patching policies.

Remember, an IoT device can be an attack vector (a weak point that can be exploited to mount an attack), a vehicle for attacks (like a part of a botnet used to carry out a DDoS attack) or a target in its own right.

Protect

Keep devices patched. The vast majority (88%) of IoT respondents said they had IoT devices in remote or difficult-to-access locations. Use over-the-air (OTA) updates to help keep these devices secure.

Harden all devices before attaching them to your network. First make sure that the device itself is tamper-resistant and tamper-evident. Then make sure that you change all default or vendor-supplied passwords. Also, reduce exposure by shutting down anything you don't need—if you're not using a port or protocol, block it.

Choose an IoT platform that enables you to deploy, monitor and manage devices easily. This can help you reduce vulnerabilities by implementing digital certificates and other security features. An IoT platform can also help mitigate attacks, for example limiting the potential damage of SIM theft by binding SIMs to devices.

Use private, non-routable IP addresses to make it harder for attackers to access IoT devices. Consider using a private cellular network to keep devices off the public internet, especially in mission-critical applications.

Encrypt data in transit and at rest. The vast majority (91%) of IoT respondents said that they are collecting PII, and 22% of those weren't encrypting it. Encrypting data can make it useless to hackers and help you mitigate the risk of a reputation-damaging data breach.

Create an IoT security assurance process that regularly analyzes IoT risk data in your organization. Ensure that users developing or purchasing IoT programs work with the information security team to factor in the cost and resources required to secure devices and applications.

Detect

An IoT platform can help you spot anomalous behavior—such as excessive data use, unusual usage patterns and access from an unexpected location—more quickly. This can help you to mitigate the damage a compromise causes.

Train staff members that see devices—this could be production line staff or field workers—to spot the signs of physical tampering.

Network visibility and monitoring are crucial to successful incident identification. This can help you see what data your IoT devices are exchanging and with whom.

Respond

Put controls in place to contain the spread of infection and prevent the attacker from gaining any additional access or access to sensitive data. This should include locking down devices or throttling down traffic when a threat is detected.

Implementing network blocks is an easy and effective way to limit an attack—stopping it from infecting more devices or the attacker from accessing more critical systems.

Recover

Conduct a post-mortem exercise to determine how the attack managed to get through and where controls, processes and technology fell short. Create and distribute an "after-action" report.

04.4 Networks and cloud

Insecure networks remain a serious threat to mobile device security. Attackers can intercept traffic through man-in-the-middle (MitM) attacks or lure employees into using rogue Wi-Fi hotspots or access points. Cloud-based services are now used for many mission-critical tasks. They are also one of the reasons that mobile devices have become more critical to business. That brings a whole new range of problems.

Quick takes

- Mobile devices make 12 Wi-Fi connections per day, on average[80]
- Four percent of users will connect to at least one risky hotspot in a year[81]
- Fifty-one percent of companies that experienced a mobile-related compromise attributed it, at least in part, to a network threat, such as a rogue base station or use of insecure Wi-Fi
- Just 8% of companies take technical measures to block the use of public Wi-Fi despite the risks
- Respondents in over a quarter (27%) of companies where the use of public Wi-Fi was banned (but not blocked) were aware that employees used it anyway

80 Wandera Threat Research. Analysis of infrastructure threats: December 31, 2019 to December 31, 2020. All active devices across entire global customer base, all verticals and regions.

81 Ibid.

Risky networks

One of the most dramatic changes that we saw in our 2020 data was the drop in the number of Wi-Fi threats encountered.

This is hardly surprising given the cancellation of most international events and travel from the start of the year and then periodic lockdowns. The fact that the number of encounters continued to fall throughout the year is likely to reflect attackers shifting to other tactics as the results of these attacks dried up.

But there's no room for complacency. Risky networks remain a threat and could well rise again as movement increases again.

The number of Wi-Fi-related threats encountered plunged.

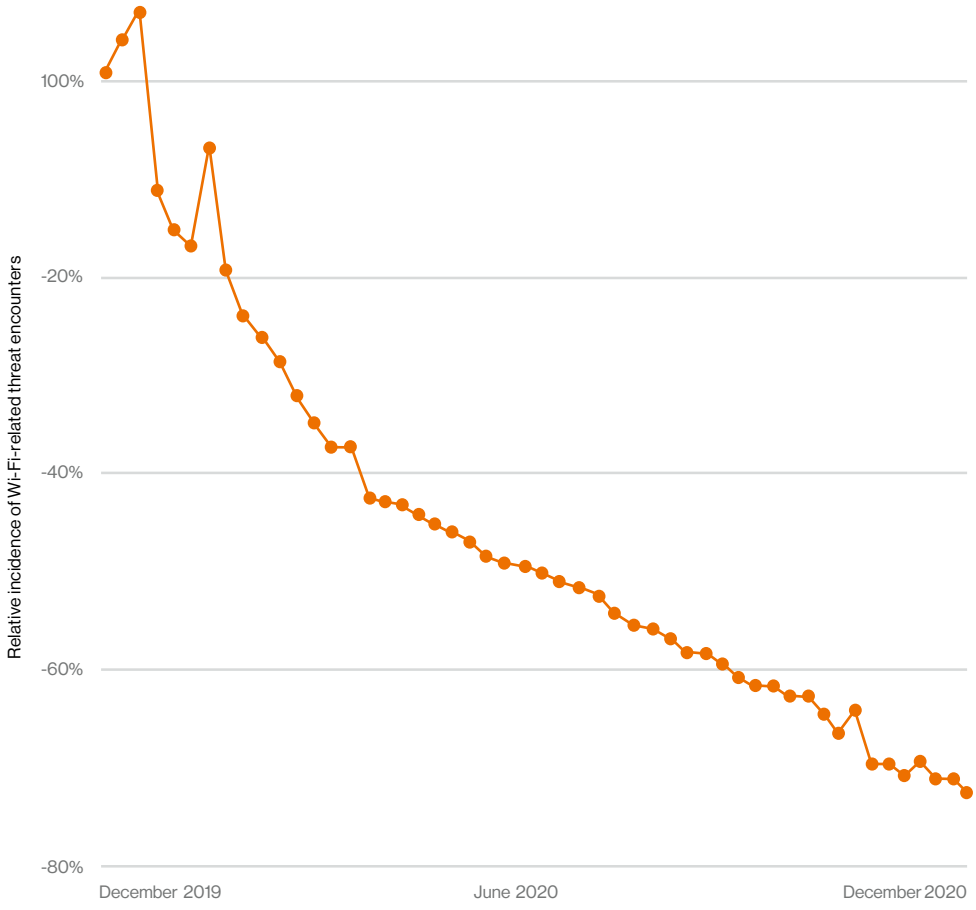


Figure 58. Relative number of Wi-Fi threat events encountered by week. Baseline 30-day period in 19Q4. Data from Wandera.[82]

82 Wandera, analysis of global customer base.

Most companies have a permissive attitude toward network use.

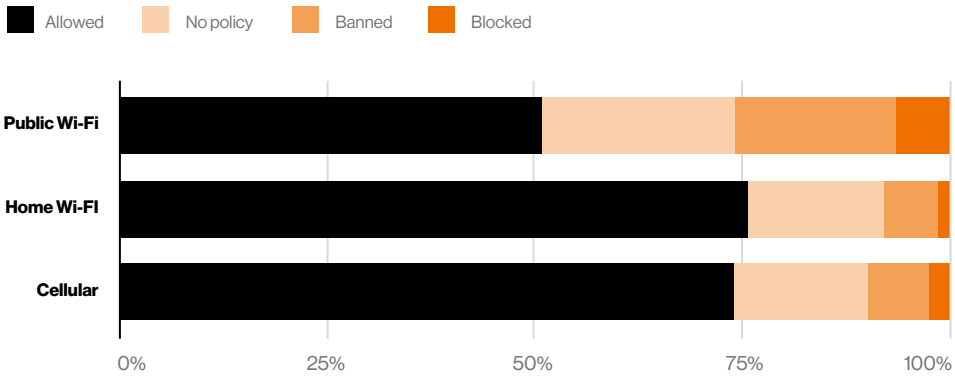


Figure 59. Which of the following do your employees use for performing work-related tasks (such as email, etc.)?

Public Wi-Fi

Despite the risks, more than half of respondents said that their company allows the use of public Wi-Fi. Nearly one in five have no policy toward it. And 18% rely solely on policy/trust. Just 8% take technical measures to block it.

Over a quarter (27%) of those organizations that ban the use of public Wi-Fi (but don't take active measures to block it) were aware that employees used it anyway. Almost half of all organizations (45%) have at least one user who connected to a risky hotspot in the previous month.[83]

Relying on trust is a questionable policy: Nearly three-quarters (71%, down slightly from 76% in the 2020 edition of this report) of respondents said they personally used public Wi-Fi for work tasks—even though 26% (up from 23%) said it was prohibited.

This may seem like a harmless infraction, but the consequences can be severe. Wandera found that each week, 4% of users connect to one or more risky hotspots.[84] This might not seem like a lot, but a single infected device could be enough to have dramatic ramifications.

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.

83 Wandera, analysis of aggregated and anonymized data from all corporate users carried out in January 2021.

84 Wandera Threat Research. Analysis of infrastructure threats: December 31, 2019 to December 31, 2020. All active devices across entire global customer base, all verticals and regions.

Respondents admitting to using public Wi-Fi themselves, even if officially banned.

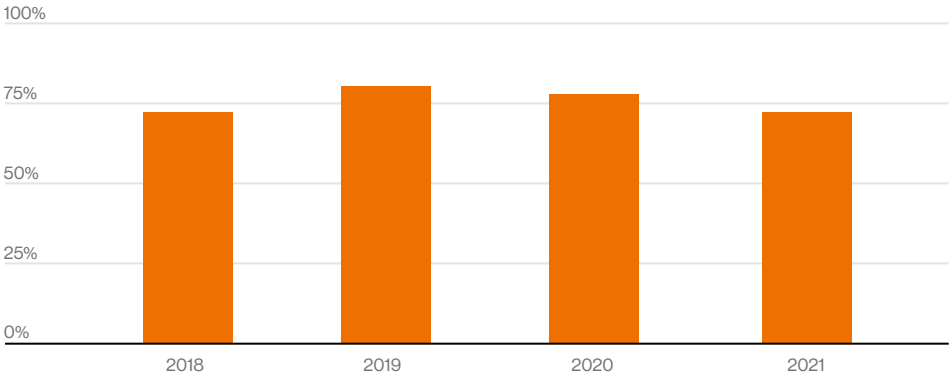


Figure 60. Do you personally ever use public Wi-Fi (e.g., in airports, coffee shops) for work tasks? [n=601, 671, 876, 856]

The dangers of public Wi-Fi are increasing as mobile devices are used for more tasks. Our respondents estimated that close to one-fifth of all data transferred back and forth between mobile devices and cloud apps is via public Wi-Fi.

Amount of data passing between mobile devices and cloud via public Wi-Fi

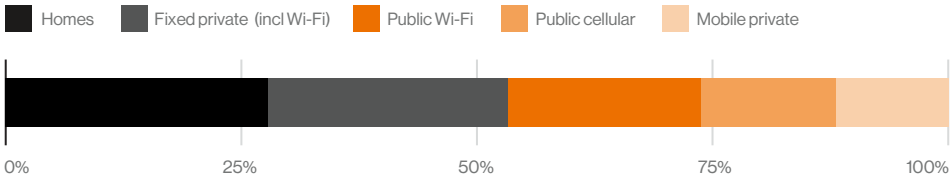


Figure 61. What percentage of your data passing between mobile devices and cloud-based services uses each of the following network types? [n=563]

In our survey, 59% of those in the retail sector (including hospitality companies) had seen rogue Wi-Fi hotspots using their business's identity.

Rogue or insecure hotspots

Not all access points can be trusted—even those carrying the name of a trusted business or brand. The risk of insecure hotspots may be greater than companies realize. Half (50%) of the organizations in our survey that suffered a mobile compromise said that a rogue or insecure Wi-Fi hotspot was involved.

According to Wandera, employees connect to an average of 24 Wi-Fi hotspots per week. It also found that 4% of devices encounter a hotspot that presents a low-to-medium severity risk, and 1% encounter one rated as a high risk—one known to be affected by MitM or a protocol attack like SSL Strip.[85]

85 Wandera Threat Research. Analysis of infrastructure threats: December 31, 2019 to December 31, 2020. All active devices across entire global customer base, all verticals and regions.

Home Wi-Fi

Bring-your-own doesn't just relate to devices. In the 2020 edition of this report, we talked about the relative safety of work, home, hotel and public networks. While home networks fared much better than public networks, they still came out as 70% more risky than company-owned and -controlled networks.

The use of employees' home networks has received additional attention since the dramatic increase in home working in the first half of 2020. In Proofpoint's 2020 State of the Phish report, it presented several concerning stats about workers' home networks, including:

- Only 31% have changed the default password on their Wi-Fi router
- Fewer than one in five (19%) have updated their Wi-Fi router's firmware[86]

VPNs

Proofpoint found that just 47% of those with a VPN installed always use it.[87] One in five never use it, or only use it when they have no other option.

Even when one's available, less than half of users always use a VPN.

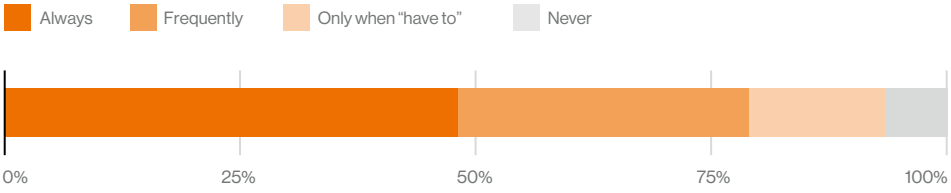


Figure 62. Employee use of company VPN. Only devices with VPN installed. Data from Proofpoint.[88]

These alarming findings reinforce the argument that security defenses shouldn't rely on user behavior. That's not accusing employees of malice or incompetence, just of being human. With nearly half of companies admitting to having knowingly sacrificed mobile device security, is it really fair or sensible to rely on every individual following all of the rules all of the time?

86 Proofpoint, State of the Phish, January 2020. A global survey of 3,500+ working adults and 600+ IT security professionals.
87 Ibid.
88 Ibid.

Cloud

Three-quarters (75%) of the respondents to our survey said that their reliance on cloud-based services is growing. Most (77%) of those said that they expected mobile device threats to grow in the year ahead (26% said that they expect them to increase significantly). And 44% of those attributed some of that growth to the increased use of cloud services and apps that store data in the cloud.

Over half (56%) of companies use web-based productivity solutions, like Google Workspace (formerly G Suite) or Microsoft 365. And most are doing at least half of their processing and data storage in the cloud.

Data stored in the cloud

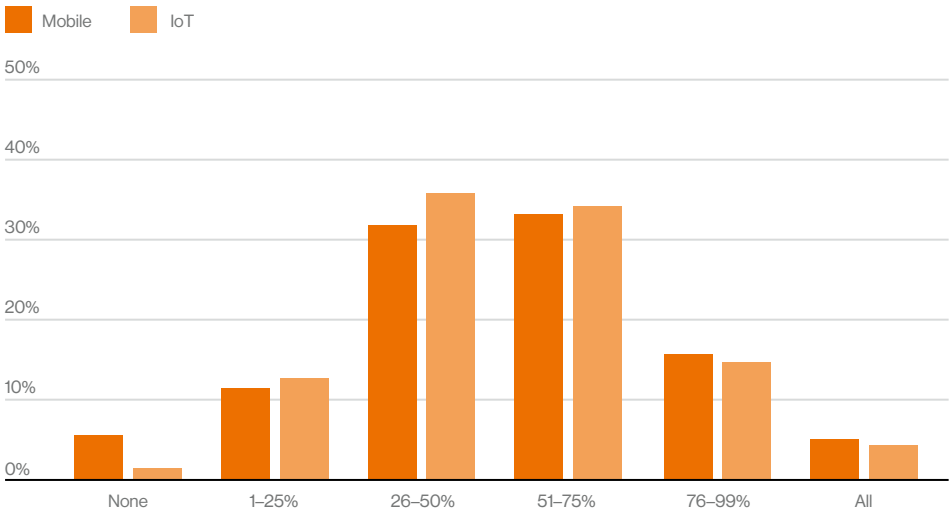


Figure 63. How much of the data that you are gathering/creating is stored in the cloud? [n=598, 258]

Processing in the cloud

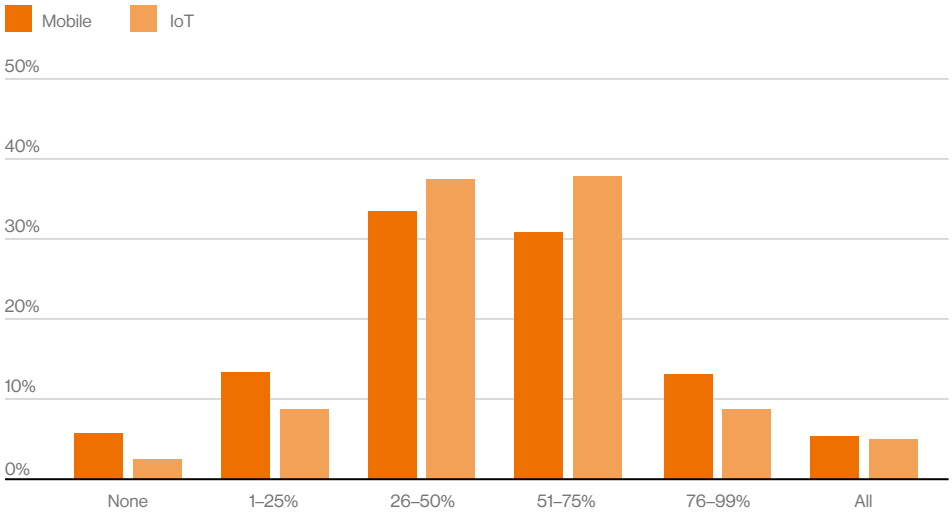


Figure 64. What proportion of your data processing is done in the cloud? [n=598, 258]

Cloud is enabling mobile workers to do more.

Part of the reason why mobile devices are more powerful tools is because of what cloud-based services enable them to do, but that's a double-edged sword. Mobile devices are also more of a target—and so more of a risk—because of what cloud services enable them to do.

Nearly half of the data transferred to and from the cloud is via home or public Wi-Fi.

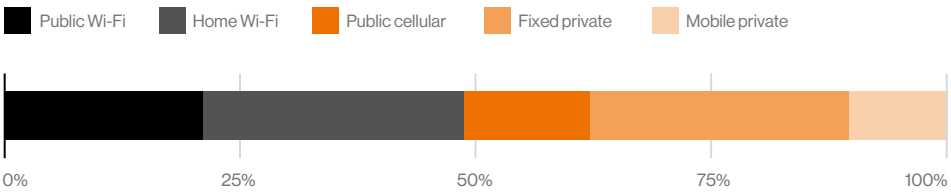


Figure 65. What percentage of your data passing between mobile devices and cloud-based services uses each of the following network types?

The number of SaaS apps in use grew again.

2019

1,295

2020

1,407

Figure 66. Average number of SaaS/web-based applications in use per company. Data from Netskope.[89]

The use of cloud apps continues to grow.

In the previous Mobile Security Index, we reported, based on analysis by Netskope, that 95% of enterprise apps and cloud services are unmanaged, with no IT administration rights or even visibility. And the number of these apps and services continues to grow. The average is up from 1,295 per company in our previous report to 1,407 in data from the second half of 2020. Some enterprises were found to have over 7,000 apps in use.

As in our previous analysis, we again found a sizable gap between the number of apps observed and the number of apps our respondents thought were in use.

There's a perception gap in the number of SaaS apps in use.

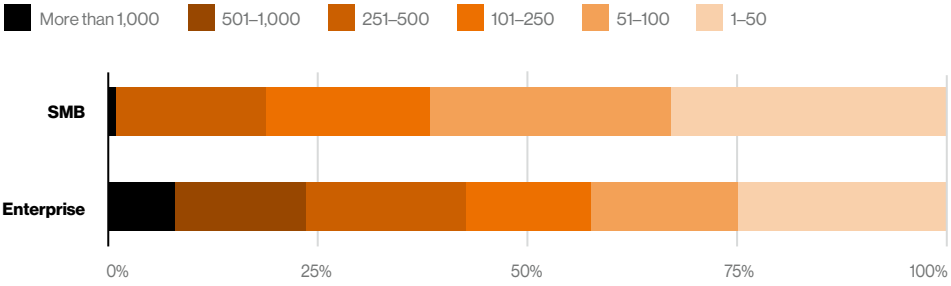


Figure 67. How many SaaS/web-based apps do your employees use? [n=598]

Nearly half of enterprise apps have a Netskope Cloud Confidence Level of "Poor," suggesting that organizations should discontinue use and migrate to safer alternatives immediately.[90]

We could explain some of this away because of the different samples and different definitions of what makes a software-as-a-service (SaaS) app. But given the size of the gap—and similarity year-over-year—it seems reasonable to conclude that companies aren't aware of just how many they have in use.

89 Netskope, January 2021. 2020 data from August to December 2020. Research was performed on anonymized usage data collected from a subset of Netskope Security Cloud platform customers that had given permission for this use.

90 Ibid.

Securing against network threats

Recommendations aligned with the NIST Cybersecurity Framework

These recommendation sections are structured around the five functions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a widely recognized model based on international standards and input from public- and private- sector organizations and academia. It provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework

Identify

Remember that it's not just the obvious stuff—like payment card data and secret plans—that you need to protect. Mobile devices could provide an entry point for a wide range of attacks. This could include attempts to disrupt operations as well as expose data. HVAC controllers are often given as an example of a system that's exploited to enter an organization and then move on to more interesting areas. That's ignoring the damage that could be done by simply messing with the HVAC system itself.

Protect

Re-architect your network into smaller segments, isolating the hosts and services that hold sensitive data. Ensure that access is granted on a "least privilege" basis. Many breaches begin with attackers exploiting vulnerabilities in systems that don't get much attention—like the corporate intranet—and then moving laterally to get to more sensitive, and potentially lucrative, data. Segmentation will make this considerably harder for them.

Secure all wireless access points. This should include only allowing known devices to connect to corporate Wi-Fi services.

Educate users on the dangers of Wi-Fi, including rogue access points. Consider putting systems like MDM or endpoint protection in place to block the use of public Wi-Fi entirely.

Because they so often use Wi-Fi or cellular networks, mobile devices are more likely to encounter MitM attacks. Implement MTD to monitor and mitigate that risk.

Look at using a remote-access VPN to secure offsite access to company resources. Make sure that employees use the VPN whenever working outside the perimeter, ideally by blocking requests from other networks.

Consider using a cloud access security broker (CASB) or secure web gateway (SWG) to help ensure that all connections to cloud-based systems are secure.

Detect

Use network intrusion detection tools to monitor all traffic, incoming and outgoing, for unusual activity. This could be an early indicator of an attack. Make sure that there's a process in place to handle any alerts promptly.

Subscribe to a threat intelligence service to get early warning of emerging threats.

Regularly analyze logs for signs of suspicious behavior. Integrating MTD with endpoint detection and response (EDR) or security incident event management (SIEM) can help simplify monitoring and, should it be necessary, forensic analysis.

Respond

If you don't have an IR plan, create one. This should cover how to qualify and categorize incidents, what should be done, and who the responsible parties are.

Speed of response is critical to limiting the damage of a security compromise. All employees should know how to raise the alarm. This is especially important when an increased share of employees are working remotely. Remember that employees may not have access to corporate systems to find out what the procedure is.

What to do in case of an incident will depend on the type of attack. It may include shutting down systems, blocking access, resetting credentials and much more.

Clear communication is important to successful IR. Your IR plan should include who to notify (including senior management, legal counsel, staff, third-party service providers and insurers), how to notify them, what to tell them and when to alert them.

Recover

Conduct a post-mortem exercise to determine where controls, processes and technology fell short. Create and distribute an "after-action" report.

If, as is quite likely, the attack involved employees using unapproved networks, consider updating your policy. At the very least, remind users about your AUP and their responsibilities.

FBI warning

Obviously, hotel bookings took a hit in 2020 as travel plummeted. But several major chains have introduced daytime bookings for those struggling with working from home and looking for a distraction-free environment.

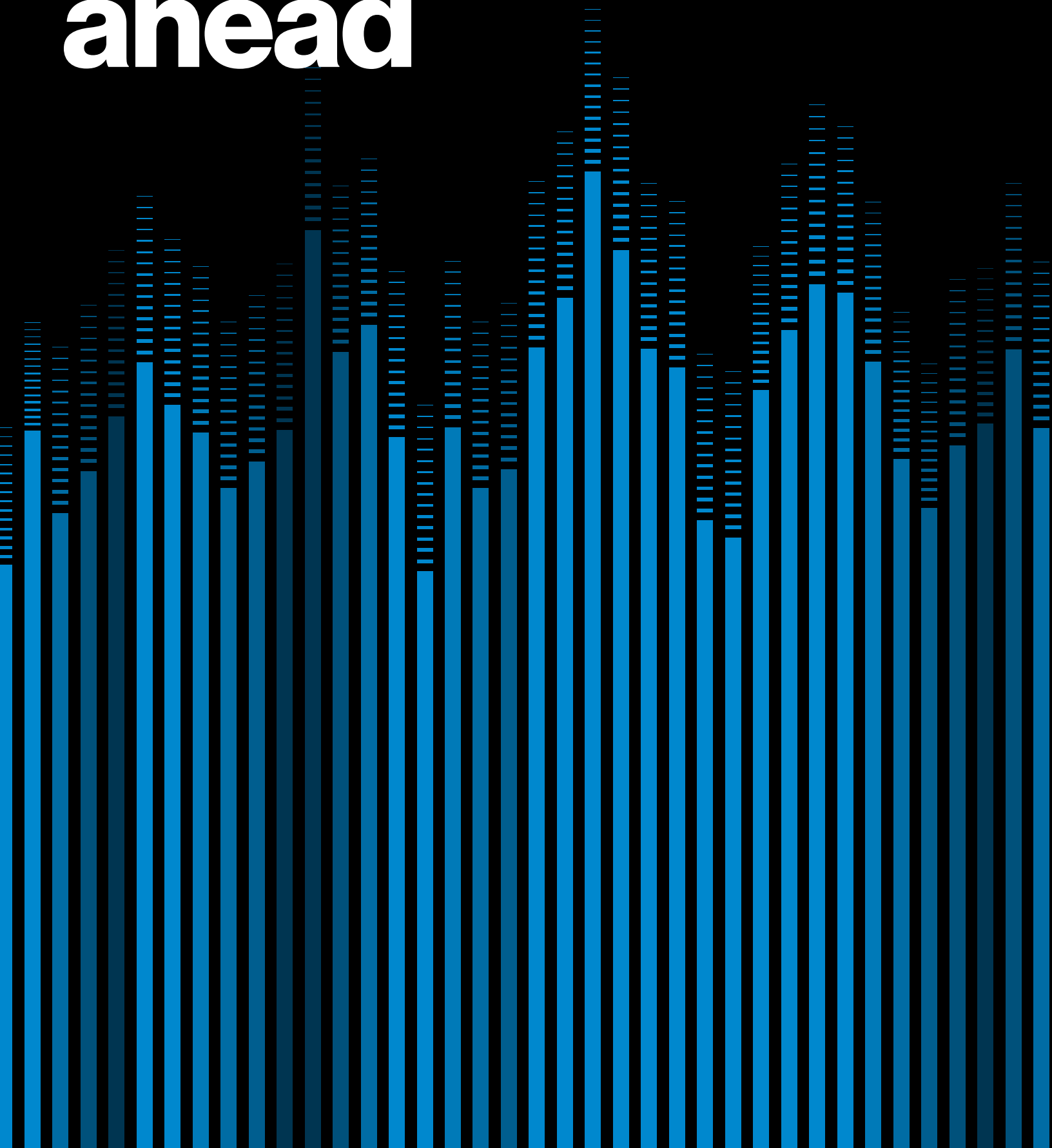
While this option may be appealing, accessing sensitive information from hotel Wi-Fi poses an increased security risk over home Wi-Fi networks. Malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests. Following good cybersecurity practices can minimize some of the risks associated with using hotel Wi-Fi for telework.

Much of a hotel's network infrastructure is entirely out of the control of the hotel guest. Guests generally have minimal visibility into both the physical location of wireless access points within the hotel and the age of networking equipment. Old, outdated equipment is significantly more likely to possess vulnerabilities that criminal actors can exploit. Even if a hotel is using modern equipment, the guest has no way of knowing how frequently the hotel is updating the firmware or that the passwords have been changed from the manufacturer's defaults, which can often be easily found online. The hotel guest must take each of these factors into consideration when choosing whether to telework on a hotel network.

For more information, see ic3.gov/Media/Y2020/PSA201006

Looking ahead

05



Drivers of change

Regulation

In the previous edition of this report, we talked about the evolution of privacy legislation. That's still a factor–almost three-quarters (73%) of our respondents said that legislation is driving action—but about as many said the same thing a year earlier (74%).

Since our 2020 report, U.S. legislators have had a general election and a pandemic to contend with. Despite this, Nevada signed new comprehensive privacy legislation[91] and Iowa, Michigan, Mississippi, New Hampshire, South Carolina, Virginia and Wisconsin joined the list of states working on such rules.[92] This means about half of Americans now live in a state where comprehensive privacy legislation has been enacted or is going through the legislative process.

IT teams are struggling to reconcile demands.

The pressure on businesses to innovate and reimagine themselves is high. It was high before COVID-19, and it's likely to be even higher afterward.

The pandemic was an outlier that many companies weren't prepared for. Even some of the best-managed, most IT-literate companies found that their business models and infrastructure weren't as resilient and flexible as they thought.

But over half (56%) of respondents said that cybersecurity challenges are holding back their digital transformation. A similar proportion (58%) said that they struggle to reconcile differing mobile demands from across the organization.

Companies said they are reassessing security in light of new regulation.

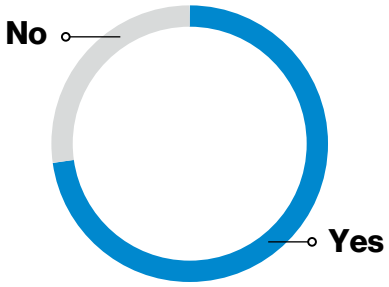


Figure 68. To what extent do you agree or disagree with the following statement? We have reassessed the risks associated with mobile devices in light of recent changes in remote working.

IT teams are struggling to reconcile differing demands.

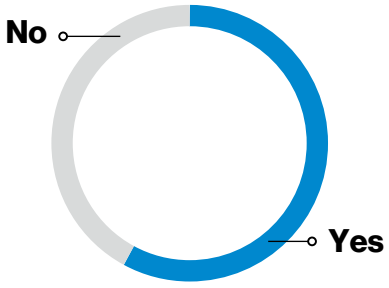
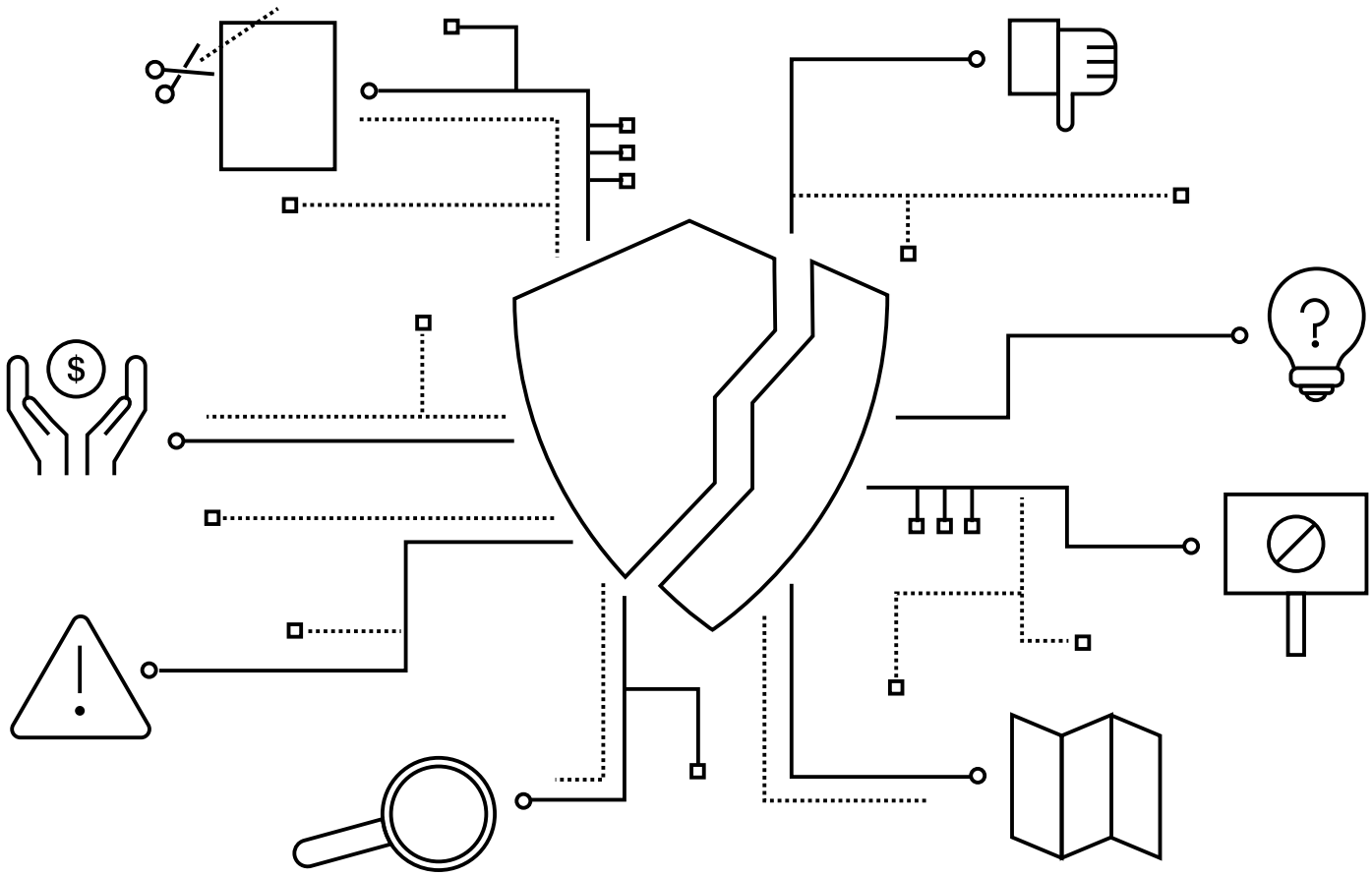


Figure 69. Do you struggle to reconcile differing mobility demands from different areas of the business?

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

92 The International Association of Privacy Professionals. https://iapp.org/resources/article/state-comparison-table/



Traditional models are broken.

We can tell that traditional security models are no longer adequate as respondents were almost as concerned about security issues caused by people going around policy for convenience as about people committing malicious acts for financial gain.

Sacrificing security for convenience was seen as one of the most common causes of compromises.

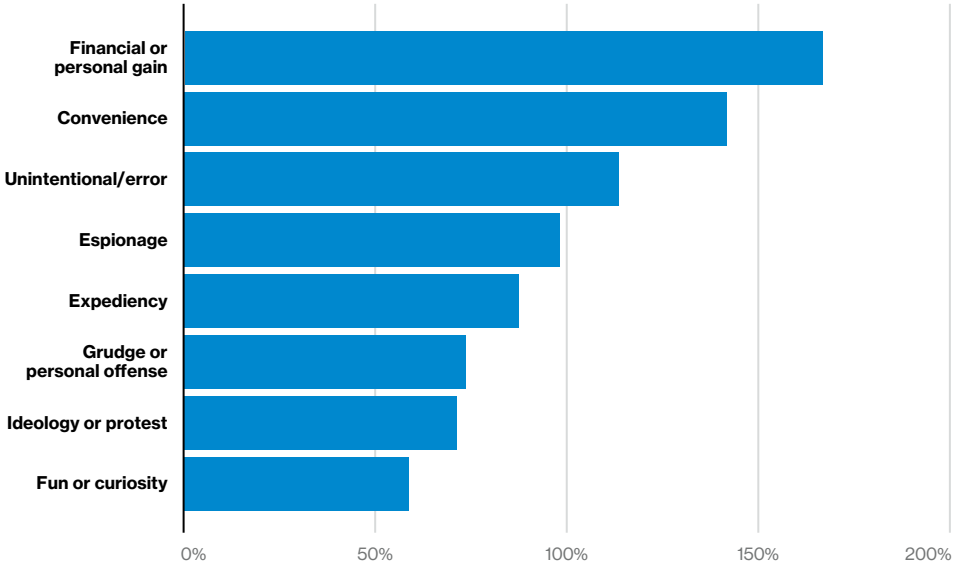


Figure 70. Which of the following underlying causes of security incidents are you concerned may affect you? Examples were given for "Expediency" (pressure from management to break rules to hit deadline) and "Convenience" (easier to go around company policy). [n=816]

The future

So long, perimeter.

It's somewhat ironic to be talking about the end of perimeters when so many people have been forced to stay at home since our previous report. The idea of the end of the perimeter isn't new. The Jericho Forum began advocating the concept of deperimeterization in 2003. It's not just the growth in the use of mobile devices that has been behind this trend; the increased use of cloud services and shift toward partner ecosystems have also driven interest.

Today, applications and data are everywhere—in company-owned data centers, in the cloud, on mobile devices and so on. Consequently, many companies struggle to maintain complete visibility into their applications and data, let alone control and manage who has access to those assets.

Many organizations have tried to overcome these issues using multiple point products, such as SWGs, firewalls and VPNs. However, with data storage and processing moving to the cloud, much traffic now bypasses VPNs and on-premises firewalls. As a result, organizations have been looking for an alternative that can accommodate both cloud and data center applications.

Zero trust network access

Many traditional security models rely on the notion of a perimeter, a bit like the old idea of a castle. The good guys are on the inside with "barbarians at the gate." In the digital world, this perimeter is enforced by VPNs, firewalls and other security devices on the edge. Once inside, there may be additional authentication required to access some resources, but you're free to wander the corridors. The paradigm could be described as "trust, but verify."

In contrast, the thinking behind zero trust network access (ZTNA) could be explained as "trust no one." Resources are hidden and only accessible through a trust broker. Even when you have obtained access to one resource, you can't even "see" other resources. As an analogy, think of a burglar breaking into a house. In the perimeter model, some of the internal doors may have additional locks. In the ZTNA model, the burglar can't even see that there are other doors.

ZTNA isn't a technology. It's often described as a security framework. It requires multiple technologies to implement. See Figure 71.

One of the big benefits is that ZTNA doesn't depend on the notion of a perimeter and so is appropriate for both on-premises and cloud-based resources. According to Gartner, 90% of those implementing ZTNA are using an as-a-service approach.[93]

Find out more.

Learn about ZTNA:

enterprise.verizon.com/en-gb/resources/articles/zero-trust-security-framework-benefits-and-downsides/

The three steps

Step	01 Verify users.	02 Validate devices.	03 Limit access.
Principle	Authenticate users when they attempt to access the system.	Confirm that all devices making requests are known, fully patched and meet minimum security standards.	Even when the user is verified and the device validated, access should only be given on a "need to know" or "least privilege" basis.
Supporting technologies	Multifactor authentication, including biometrics and one-time passcodes	Endpoint device management and digital certificates	Network segmentation and software-defined perimeter

Figure 71. The three steps of ZTNA.

93 Gartner, Market Guide for Zero Trust Network Access, June 2020.

Secure access service edge

Secure access service edge (SASE, pronounced “sassy”) is also not a security technology. It’s an architecture—originally proposed by Gartner, a leading research and advisory firm—that is designed for the mobile-first and cloud-first world.

It reflects the decentralized architectures that companies now operate or are moving toward. It integrates network and security services into a single, distributed, cloud-centric solution that protects all traffic, applications and users. It encompasses ZTNA, CASB, DLP and much more.

This approach helps organizations deploy, manage and scale infrastructure securely. Its flexibility makes it easier for companies to scale their security infrastructure as they grow, without having to reconfigure the central architecture. The SASE model also enables organizations to support on-premises and cloud-based applications without requiring separate infrastructure as with conventional proxy- and software-defined-perimeter-based solutions.

It’s still early days.

ZTNA and SASE are both relatively new concepts and, accordingly, adoption is still low. However, 80% of organizations said they are more likely to evaluate a ZTNA solution as a result of the events of 2020.[94]

North America leads in the adoption of ZTNA.

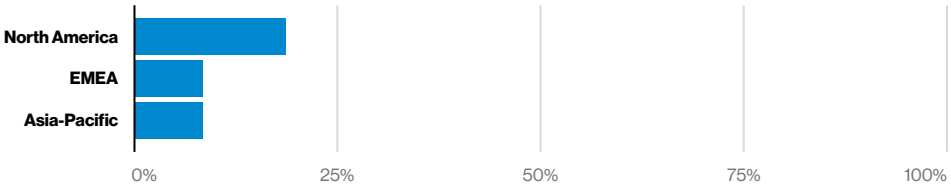


Figure 72. Companies taking a ZTNA approach by region. Data from Asavie.[95]

Asia-Pacific lags in the adoption of SASE.

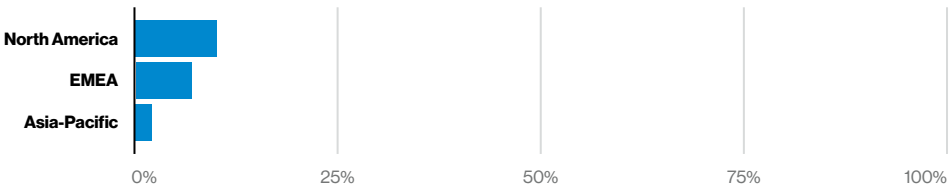


Figure 73. Companies that have adopted SASE by region. Data from Asavie.[96]

94 NetMotion, SDP report, June 2020. A survey of over 600 network and IT professionals across the U.S., the U.K. and Australia.

95 Asavie, The Future of the Secure Office Anywhere, October 2020. Based on detailed interviews with 1,005 key business stakeholders, including C-Suite, IT and cybersecurity leaders, across North America, EMEA and Asia-Pacific.

96 Ibid.

Conclusion

It's highly unlikely—especially if you are reading it soon after its release—that you are reading this report in "the office." And if you are reading a digital copy, it's pretty likely that you downloaded it over a wireless network—quite possibly one not owned or controlled by the organization that you work for. That's the reality of the modern workforce.

Much has been said about the impact of COVID-19 on working practices, but things have been changing for many years. Mobile devices are a fundamental part of this. As devices have become more powerful, aided and abetted by cloud-based services, companies have found more ways to make use of them. And that cycle continues; 5G promises to unleash a whole new wave of innovation.

Unfortunately, as devices have grown more powerful, they've become more appealing to those with malicious intentions. Solutions have evolved, but, as we've seen, even when tools are in place, people don't always use them. Part of the problem is the gulf between how mobile devices and remote workers have been treated compared to others.

Recently, new security models that recognize the mobile-first, cloud-first reality of modern business have emerged. These promise to make mobile device security better for all concerned: the company that wants to protect valuable systems and data; the admins that have to manage and secure devices; and the users that depend on these devices to be productive. It's still early days, but we expect these models to rapidly gain ground.

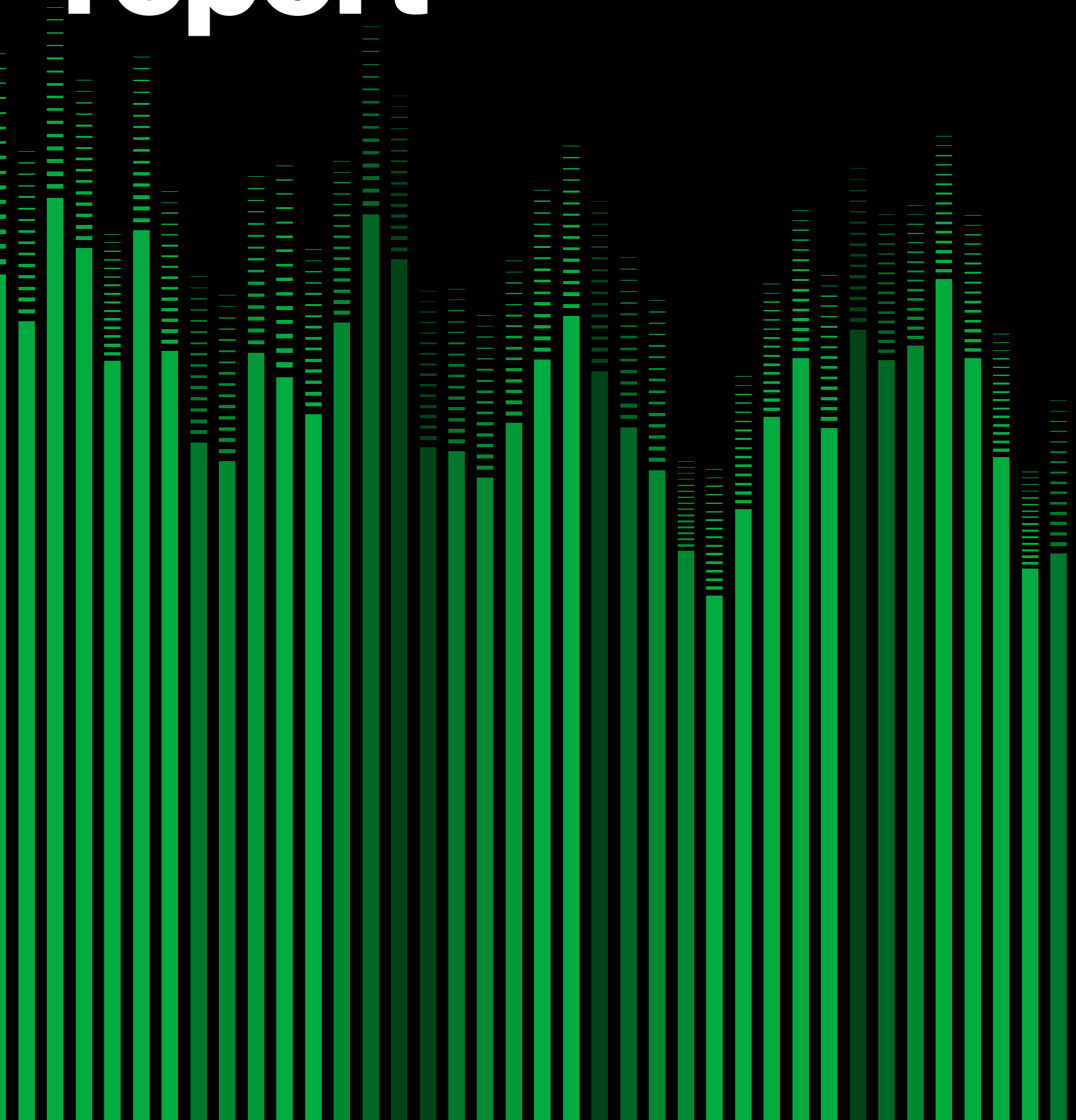
Much as how mobile devices are managed and secured in merging with other devices, there remain distinct differences between how these devices are used. In the past, terms like "home worker" and "mobile worker" have been used interchangeably. As the world recovers from the COVID-19 pandemic and working patterns settle to a new normal, we expect the important differences between working personas to become more evident. There's a lot of work to do in bringing processes and policies up to date for what lies ahead.

All this raises the question of whether there will be a need for a Mobile Security Index 2022? In many ways, that's down to you, our readers. We'd love to hear whether you've found this report useful and how you see mobile device security changing. Tell us which findings you've found interesting and which you disagree with. Let us know what we've missed and what you'd like to see in the future.

Tweet @VerizonBusiness with the hashtag #cybersecurity.

About this report

06



Terminology

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

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

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

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

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

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

Incident
This covers any form of security event, malicious or not, successful or not. This could be anything from a failed authentication attempt to a successful compromise and data breach. It 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 of data. This can apply to a technique, such as phishing, or an actor, such as an organized criminal group.

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

Breakdown of respondents

Mobile respondents by country

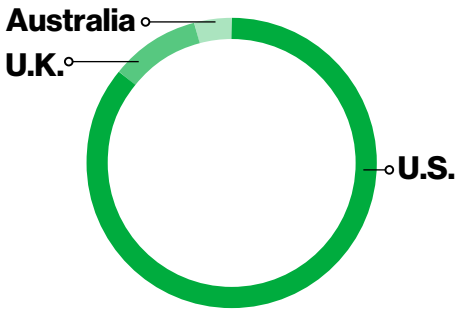


Figure 74. In which country are you based? [n=598]

IoT respondents by country

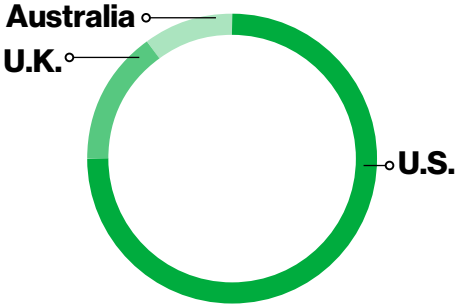


Figure 75. In which country are you based? [n=258]

Survey methodology

Mobile respondents by company size

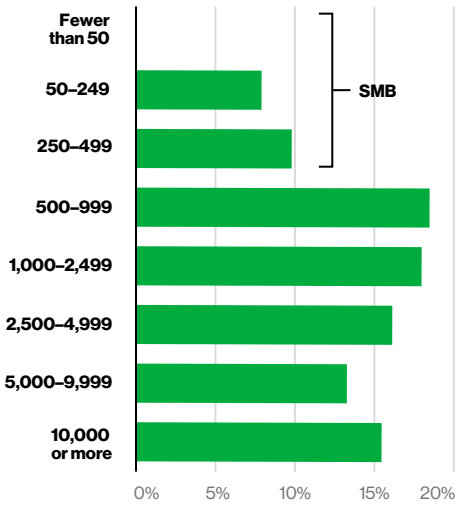


Figure 76. How many employees does your organization have? [n=598]

IoT respondents by company size

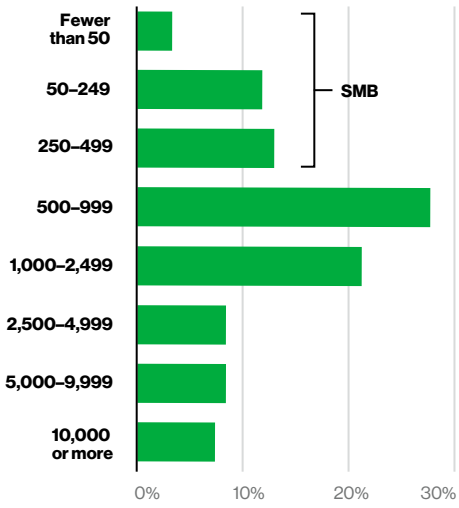


Figure 77. How many employees does your organization have? [n=258]

Mobile respondents by industry

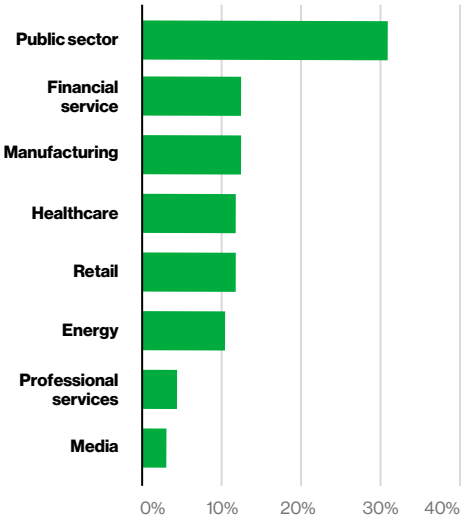


Figure 78. Which industry sector best describes your organization's primary activities? [n=598]

IoT respondents by industry

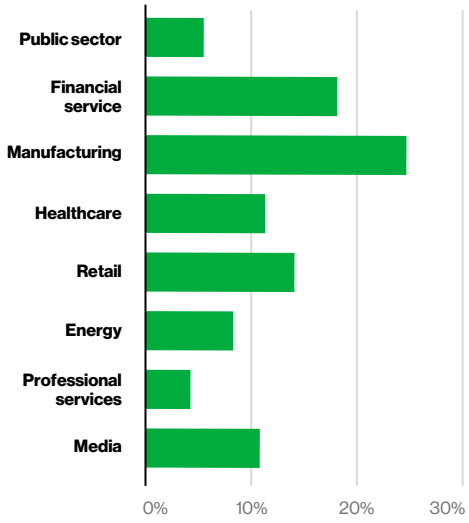


Figure 79. Which industry sector best describes your organization's primary activities? [n=258]

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

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

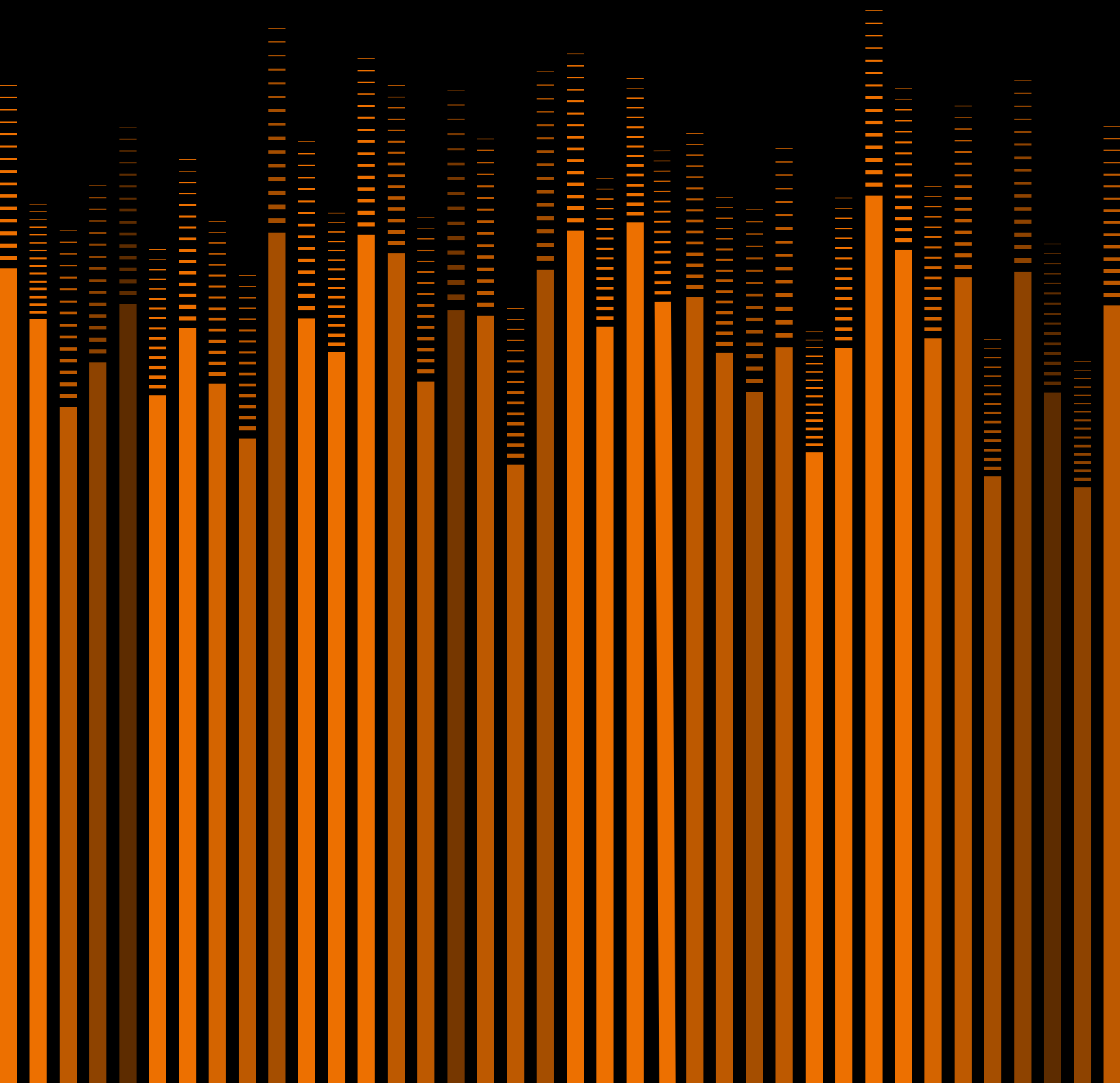
Our sample included both small companies and large enterprises. Company size was not a strong indicator for most of our questions. Unless stated otherwise, all data in this report is from this survey.

Unless stated otherwise, stats quoted in this report are from the mobile respondents.

Partner contributions

Details of the source of data and statistics supplied by our contributors are given in the next section.

Contributors 07



Security companies

Asavie, an Akamai company

Asavie simplifies digital transformation for enterprises and OEMs, including the most advanced IoT and enterprise software-defined wide area network (SD-WAN) deployments. Its self-serve, programmable SaaS solutions enable secure mobile access in a multi-cloud, multi-network world. It unifies visibility and control across all of an organization's mobile and IoT endpoints, as well as legacy greenfield implementations, providing intelligent insights to help reduce costs and improve overall performance. It is an ISO-27001 certified company.

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

asavie.com

Check Point

For the last three decades, Check Point Software Technologies has set the standard for Cyber Security. Our mission is to secure your everything. Across the ever-evolving digital world, from enterprise networks through cloud transformations, from securing remote employees to defending critical infrastructures, we protect organizations from the most imminent cyber threats.

Check Point is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from fifth-generation cyber-attacks with an industry-leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

With over 3,500 security experts, a world-acclaimed research and intelligence unit, and the broadest ecosystem of business and technology partners, we protect over 100,000 organizations of all sizes across all industry verticals in 88 countries to achieve better experiences in a safer digital world.

checkpoint.com

Blackberry Cylance

BlackBerry Cylance provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500 million endpoints including more than 175 million cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear: to secure a connected future you can trust.

blackberry.com

MaaS360

IBM

IBM Security MaaS360 with Watson transforms how IT is securing smartphones, tablets, laptops, desktops, wearables and IoT without sacrificing a great user experience. Artificial intelligence (AI) and predictive analytics keep you alerted to potential endpoint threats and provide remediation to avoid security breaches and disruptions. MaaS360 protects apps, content and data so organizations can rapidly scale their remote workforce and BYOD initiatives.

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

ibm.com/security/mobile/maas360

Lookout

Lookout

Lookout is a leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, enterprises, government agencies, and partners such as Verizon, Microsoft, Google, and Apple.

Powered by the largest data set of mobile code in existence, the Lookout Security Graph provides visibility into the entire spectrum of mobile risk. The installed base of Lookout's personal and enterprise mobile endpoint products is over 200 million mobile devices worldwide. This acts as a global sensor network that provides visibility into the threat landscape, including over 140 million apps—and that's growing by up to 90,000 apps a day.

lookout.com

MobileIron, acquired by Ivanti

The Ivanti automation platform makes every IT connection smarter and more secure across devices, infrastructure and people. From PCs and mobile devices to virtual desktop infrastructure and the data center, Ivanti discovers, manages, secures and services IT assets from cloud to edge in the everywhere enterprise—while delivering personalized employee experiences. In the everywhere enterprise, corporate data flows freely across devices and servers, empowering workers to be productive wherever and however they work. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world.

ivanti.com

NetMotion

NetMotion provides security solutions for millions of devices deployed around the world, including 7 of the 10 largest airlines, 85% of U.S. public safety agencies, and a variety of other major organizations. Customers choose the NetMotion platform for its powerful software-defined perimeter (SDP/ZTNA), experience monitoring and enterprise VPN functionality. NetMotion stands out for its ability to improve the employee experience, validated by a satisfaction rating of 97% and a net-promoter score (NPS) of 91. NetMotion is headquartered in Seattle, with offices in Victoria, Chicago, London, Tokyo, Sydney and Frankfurt.

netmotionsoftware.com

Netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

netskope.com

Proofpoint

Proofpoint, Inc., is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web.

proofpoint.com

Qualcomm

Qualcomm is the world's leading wireless technology innovator and the driving force behind the development, launch, and expansion of 5G. When we connected the phone to the internet, the mobile revolution was born. Today, our foundational technologies enable the mobile ecosystem and are found in every 3G, 4G and 5G smartphone. We bring the benefits of mobile to new industries, including automotive, the internet of things and computing, and are leading the way to a world where everything and everyone can communicate and interact seamlessly.

qualcomm.com

Thales

Thales is a global high technology leader investing in digital and "deep tech" innovations—connectivity, big data, artificial intelligence, cybersecurity and quantum technology—to build a future we can all trust, which is vital to the development of our societies. The company provides solutions, services and products that help its customers—businesses, organizations and states—in the defense, aeronautics, space, transportation, and digital identity and security markets to fulfil their critical missions, by placing humans at the heart of the decision-making process.

thalesgroup.com

VMware

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

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

vmware.com

Wandera

Wandera provides a zero-trust cloud security solution to protect the modern workplace. We enable zero-trust access to all your applications, secure your data and devices against cyber threats, and help you apply policies to filter internet access and reduce risk exposure. We believe in making security simple. This is why we created a unified offering, managed through a single console and supported by the broadest range of ecosystem integrations. Wandera is recognized as a leader by analyst firms. Today, we work with thousands of customers that are serviced through our fast and scalable global network.

wandera.com

Law enforcement

Europol

Europol is the European Union's law enforcement agency. Its main goal is to achieve a safer Europe for the benefit of all the EU citizens. Headquartered in The Hague, the Netherlands, it supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organized forms of crime. It also works with many non-EU partner states and international organizations.

europol.europa.eu

Federal Bureau of Investigation (FBI)

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

fbi.gov

United States Secret Service

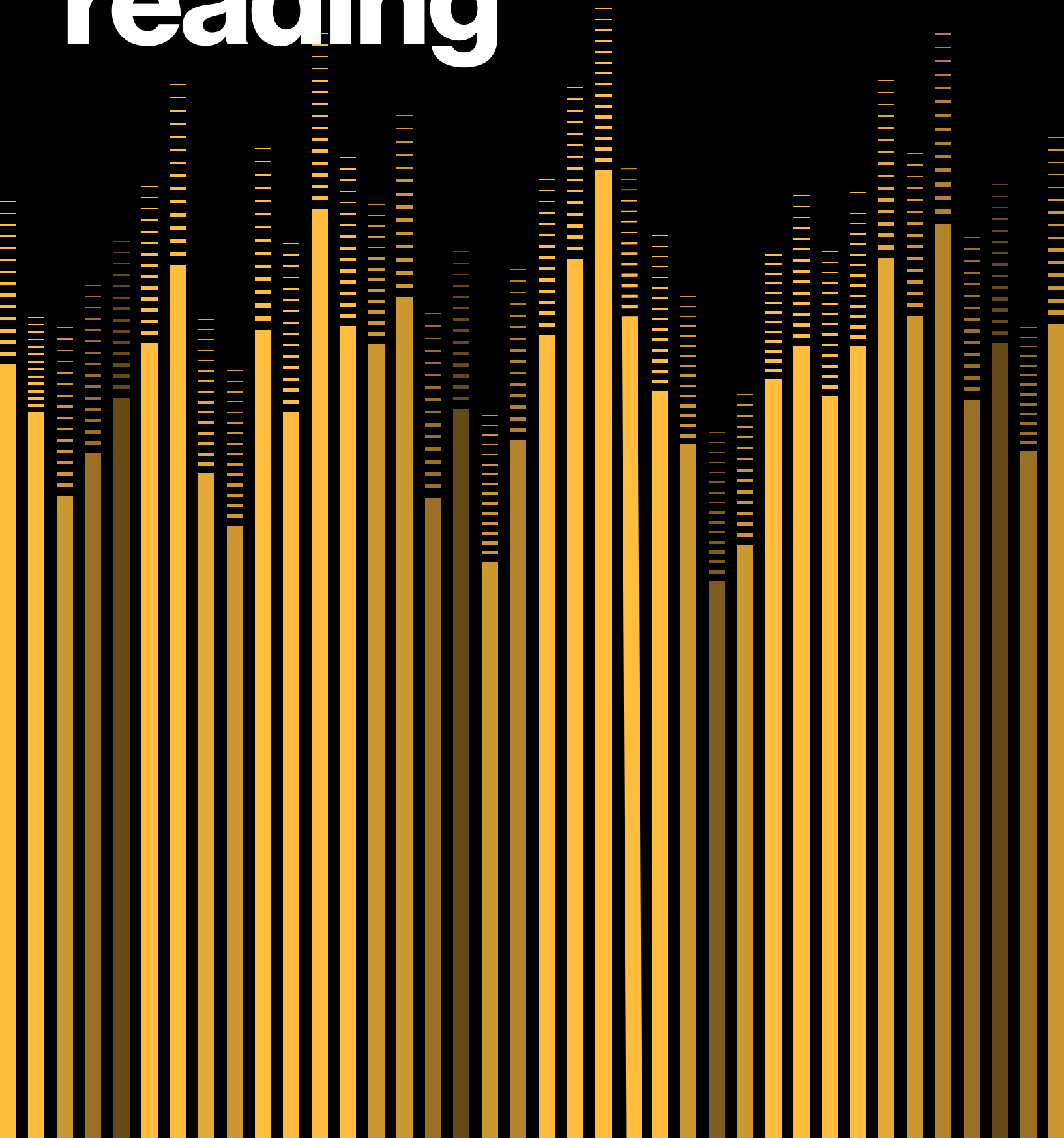
The U.S. Secret Service has two core responsibilities: ensuring the safety of the U.S. President and Vice President, their families, and other designated individuals, events and locations; and safeguarding the nation's financial and payment systems. While the Secret Service is undeniably today better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

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

secretservice.gov

Further reading

08



Verizon thought leadership

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

Other Verizon Mobile Security Index publications

Industry spotlights

These concise reports provide detailed insights into the state of mobile security in four key vertical sectors:

Financial services

enterprise.verizon.com/msi-financial-services

Healthcare

enterprise.verizon.com/msi-healthcare

Retail

enterprise.verizon.com/msi-retail

Manufacturing

enterprise.verizon.com/msi-manufacturing

Small and medium-sized business spotlight
This report gives a deep dive into the threats companies with up to 499 employees are facing.

enterprise.verizon.com/msi-smb

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

enterprise.verizon.com/msi-public-sector

Other Verizon security reports

Data Breach Investigations Report

The Data Breach Investigations Report (DBIR) is one of the IT industry's foremost security publications. Since 2008, it has provided highly respected insight into the state of cybersecurity based on analysis of real incidents. Overall, the DBIR team has analyzed over 375,000 security incidents, including nearly 18,000 confirmed data breaches, from around the world. The 14th edition will be published in mid-2021.

verizon.com/dbir

Cyber-Espionage Report

The Cyber-Espionage Report is a data-driven publication that focuses on advanced cyberattacks as reflected in the DBIR "Cyber-Espionage" incident classification pattern. It sheds light on the state of cyber-espionage based on analysis of seven years (2014–2020) of DBIR data. This includes identifying the threat actors and the tactics, techniques and procedures they use. Just as importantly, it identifies the victims, attributes, assets and data they target and details what can be done to prevent, mitigate, detect and respond to attacks.

verizon.com/business/resources/reports/cyber-espionage-report/

Payment Security Report

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

verizon.com/paymentsecurityreport

Additional resources from government and law enforcement agencies

FBI advisories on BEC

Read the FBI's statistics on the rise of reported incidents of business email compromise (BEC) fraud around the world. Learn about total reported losses and how to protect your own organization.

fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

FBI advisories on ransomware

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

fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Mobile security updates from NIST's Center of Excellence

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

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

USSS Preparing for a Cyber Incident

Prepare for the inevitable with this guide from the U.S. Secret Service (USSS). It describes what organizations should do to build an understanding of the technological and regulatory limitations, responsibilities and resources available to them, and how to apply that knowledge to their operations.

secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

NIST guidance on COPE devices

Get helpful guidance on managing corporate-owned personally enabled (COPE) mobile devices and reducing the risk these devices can pose to cybersecurity.

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

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

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

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