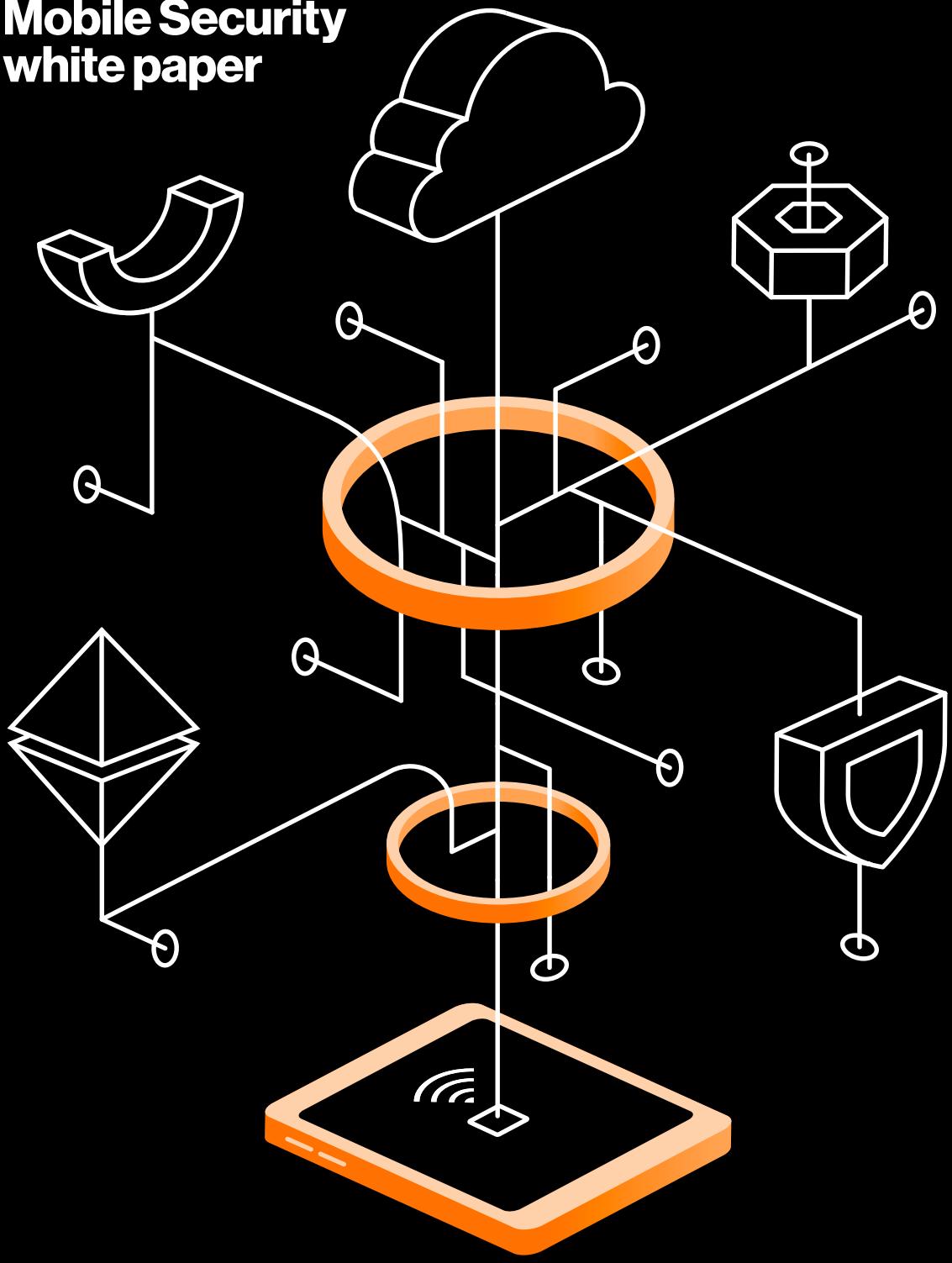
MSI

2023 Mobile Security Index white paper



verizon

Who should read this white paper?

We produced this Verizon Mobile Security Index white paper to help security professionals, such as chief information security officers (CISOs), assess their organization's mobile security environment and calibrate their defenses. This report is also relevant to anyone involved in the specification, procurement or management of IT devices and services.

Definitions

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

Attack	A general term covering any deliberate unauthorized action toward a system or data. 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	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.

Contents

Introduction

The statistics are sobering: 61% of CISOs (and 53% of CEOs) think that their organization is unprepared to cope with a targeted cyberattack in the next 12 months.[1] With mobile devices now making up a large part – even the majority – of the device estate, mobile security is more important than ever.

Those managing security must protect a growing number and diversity of endpoints. Increasingly, those endpoints are mobile or using mobile connectivity. Bring-your-own-device (BYOD) policies, hybrid working and the proliferation of Internet of Things (IoT) have multiplied the scale and complexity of protecting endpoints. This ultimately affects the business, its employees, shareholders and customers.

In this report, we'll look at some of the biggest threats to mobile devices – from the phone in your pocket to the predictive maintenance sensors on a 5-ton steel press.

In the 2022 edition of the Mobile Security Index, we reported that nearly two-thirds (66%) of respondents said that they'd come under pressure to sacrifice mobile device security "to get the job done." Of those, 79% (or 52% of all respondents) had succumbed to that pressure. In this white paper, we look at the challenges of balancing security with user experience, privacy, freedom and cost. We offer some guidance on how to strike this balance.

According to Forrester, IoT devices, employee-owned mobile devices followed by company-owned mobile devices were the three most common targets in external attacks.

Forrester[2]

1 Proofpoint, Cybersecurity: The 2023 Board Perspective, 2023
2 Forrester, The State Of IoT Security, 2023

What's at risk?

One of the reasons why mobile devices likely don't get the attention that they deserve is that people focus on what's on the device. But it's not just what's on the device that businesses have to worry about. As of 2022, 60% of all corporate data was stored in the cloud.[3]

Mobile phones make an attractive target in a similar way to a wallet. Pocketing the cash might be nice, and maybe all an attacker is after. But it's the cards that offer access to much greater rewards for attackers that know what they're doing. The content stored on a phone may be of some interest, but the greatest potential value of compromising the device is the entry point it could offer to the company's "crown jewels" – its customer data, intellectual property and other secrets. And many of the characteristics of mobile devices make them more vulnerable than other assets, namely:

4 cons of mobile device security

Convenience

The portability of mobile devices – obviously not the aforementioned steel press – can make them easier to steal.

Connections

Mobile devices typically connect to more networks – often insecure public ones. This can expose them to more risk.

Control

Organizations often have less visibility of mobile devices and they're often less well-protected than endpoints like servers.

Content

Users often blur the lines between work and personal tasks when using mobile devices – and what apps and data they store on them.

So why aren't mobile device breaches constantly in the news? While cybersecurity is much bigger news than it was a few years ago, companies are often reticent to share the details of attacks they've suffered. Even when details are discussed, it's rare that the specific device type involved in the initial compromise is mentioned.

It's a lot like when a company wins a big deal. Very few companies are able to trace back all the points of contact or all the little things that encouraged the customers to place the order – such as the marketing emails, TV ads, events, etc. Likewise, a breach may be attributed to a phishing attack, but maybe that only worked because the message came from a legitimate address. So, an earlier credential-stuffing attack was actually a critical step in the attack.

"Various studies estimate that as many as 90% of successful cyberattacks and as many as 70% of successful data breaches originate at endpoint devices.[4]

91%

of CEOs/CFOs put the responsibility for cybersecurity squarely with IT.

Accenture[5]

3 Lookout, The State of Remote Work Security, 2023
4 IBM, What is Endpoint Security?, 2023
5 Accenture, Elevating the Cybersecurity Discussion, 2022

Plenty of stones left unturned

Unsurprisingly, headlines about security breaches tend to focus on the impact – the number of customers affected, the disruption to services, the cost of remediation and the fines levied. Many security reports focus on the techniques employed to gain access to systems and data. What isn't discussed very often is what happens between when a company's systems are first compromised and when the attackers' presence is detected. Over the years, the authoritative source of cybersecurity breach information, the Verizon Data Breach Investigations Report (DBIR), has tracked how long it takes companies to discover a breach.

Detection in non-actor-disclosed breaches errors

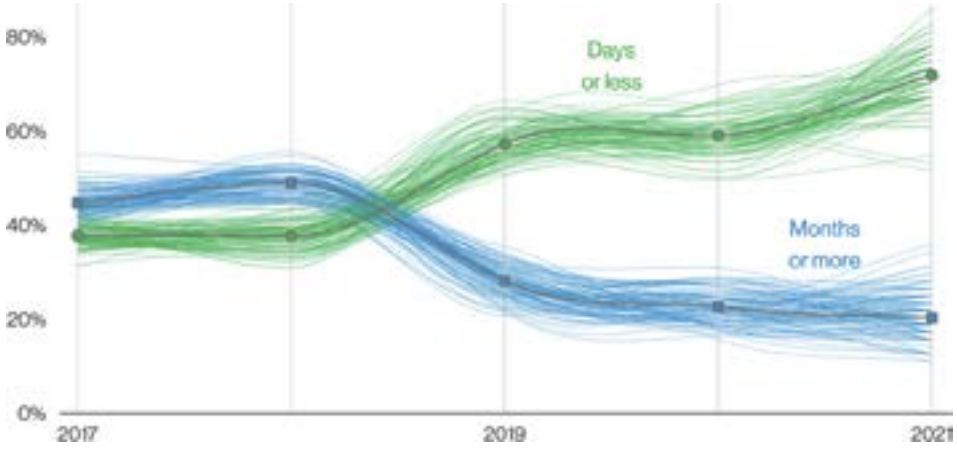


Figure 1: Time to detect intrusion (non-actor disclosed breaches).[6]

Around 50% of intrusions are disclosed by the perpetrators – who either send a ransomware demand, brag about their success on a forum or put the loot up for sale. Around one-fifth goes undiscovered for months or more.[7]

It wasn't until the 1970s that the Allies admitted that they'd broken the German Enigma machine in 1941. If they'd let the Nazis know they could read their messages before the end of World War II, they'd have stopped using the machine and an incredibly valuable source of information would have dried up. Likewise, cyberattackers often lurk in the shadows gathering useful intelligence and nosing around.

It's an effective tactic. According to IBM, nearly 40% of the data breaches that it studied involved the loss of data from across multiple environments – including public cloud, private cloud and on-premises. This shows that attackers were able to move laterally and compromise multiple environments before being detected.[8]

4 ways attackers can exploit access

Persistence

Lying low and staying alert can yield results. Eavesdropping for an hour may prove pretty boring. Eavesdropping for a couple of months is much more likely to reveal something valuable or useful in an attack.

Lateral movement

Like a burglar moving from room to room, cybercriminals will often use the access they've gained to move from system to system until they find something valuable.

Impersonation

Today, many staff are wise to the dangers of social engineering. But even technologically savvy employees may fall for an email or instant message "from a colleague." Attackers can exploit this to access other systems, change payment details and more.

Credential elevation

Similar to lateral movement, attackers can use a set of compromised credentials to compromise other credentials – perhaps using impersonation – with greater access.

6 Verizon, Data Breach Investigations Report (DBIR) 2022
7 ibid.
8 IBM, Cost of a Data Breach Report 2023, 2023

Users and behaviors

The enormous increase in the functionality of mobile devices has fundamentally altered how we think about work. It's changed the way we think about where we work from, as well as how we separate work and personal – both activities and responsibilities.

In the 2022 Mobile Security Index, we discussed how the world has moved from "work from anywhere" to an "everywhere, all the time" mindset. While this shift may have improved productivity – although there is some debate – it has also created additional challenges for IT and security teams.

The first challenge is that the separation between work and personal device use has all but evaporated. Who doesn't occasionally check messages or do some shopping on a work device? Most users don't even consider that something "harmless," like using personal social media or connecting to an unknown Wi-Fi network while traveling, could impact their entire organization.

The majority of data breaches involve a human weakness, often people falling for social engineering techniques.

The complacency problem

Despite improvements in cybersecurity training over the years, many users are not well-informed about the risks associated with mobile devices. Nearly half (49%) of users think that clicking on a malicious link or opening a malicious attachment can only affect their device.[9]

That helps explain why over a third (34%) of users have fallen for one of the five following basic security errors.

5 basic security errors

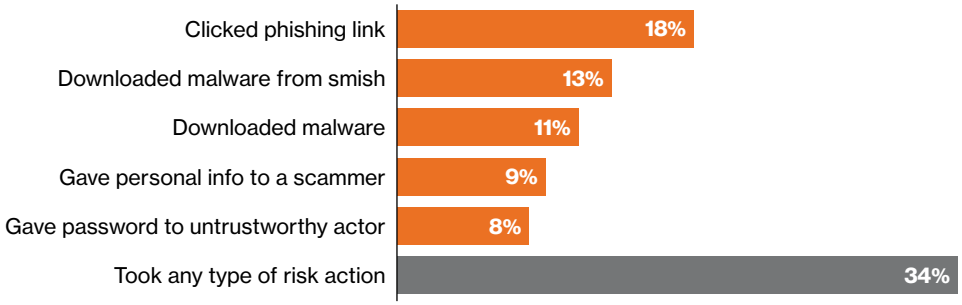


Figure 2: Risky behaviors exhibited by users. Proofpoint[10]

A lack of understanding of the potential consequences combined with the blurring of boundaries between home and work make a dangerous combination.

81%

of organizations faced malware, phishing, and password attacks last year which were mainly targeted at users. This underscores that employees can be an organization's weakest point.

Fortinet[11]

9 Proofpoint, State of the Phish 2023, 2023
10 ibid.
11 Fortinet, 2023 Security Awareness and Training Global Research Brief, 2023

The danger of security fatigue

Fatigue is a serious concern. Let's face it, having to remember and enter passwords is boring. Having to be constantly vigilant is tiring. People have a lot to think about.

The risks of security fatigue are demonstrated by the increase in cyber-insurance claims connected with multifactor authentication (MFA) spamming attacks. According to cyber-insurance group Coalition, these have been steadily growing since September 2022.12

A false sense of security

MFA is supposed to help improve security. But as we've discussed in previous reports, it's not a panacea. In fact, the false sense of security that having MFA in place can generate is a risk in itself.

Increasingly SMS- and authenticator-app-based types of MFA are being supplanted. Many applications now use a form of MFA where users are asked to respond – typically accept or reject – to an alert on their mobile device. In an MFA spamming attack, the perpetrator bombards the user with prompts in the hope that the person will click "accept" to make the annoyance go away. Some do.

In 2022, Uber suffered a high-profile – although, it said, fairly harmless – breach due to MFA fatigue.[13] The attacker used a contractor's compromised VPN credentials to repeatedly attempt to log in. When this didn't succeed, the attacker contacted the victim on WhatsApp and, pretending to be Uber IT support, encouraged the employee to accept the request. They did. The attacker was able to exploit access to the VPN to move laterally to breach critical systems such as the company's email, cloud storage and code repository.

Uber was not the only target. In response to these attacks, Microsoft issued an update that requires users responding to MFA push notifications to input a number that appears on the screen of the device that is trying to log in. The update also adds additional context to requests, including application name, device location and IP address. Okta and Duo have followed suit with similar updates.

74%

of all breaches include the human element.

Verizon 2023 DBIR[14]

Even as organizations spend billions every year to shore up their infrastructure, they may be neglecting the people-based security risks that matter most. People are the easiest and most lucrative entry point into your environment.

Proofpoint[15]

12 Coalition, MFA spamming attacks increase cyber claims, 2023
13 Lookout, Social Engineering and VPN Access: The Making of a Modern Breach, 2022
14 Verizon, Data Breach Investigations Report (DBIR) 2023, 2023
15 Proofpoint, The Definitive Email Cybersecurity Strategy Guide, 2022

Is working from home here to stay?

Not long ago it seemed like working from home could become the norm. Immediately after lockdowns were lifted, users were reluctant to return to the office. But now, lots of companies – even some of those that benefited most from the increase in remote working – are now encouraging – in some cases forcing – workers back to the office.

According to research by Ivanti, nearly half of knowledge workers are now back in the office. Interestingly, it found that the C-suite was most likely to be following a hybrid model – 60% of respondents.

Current working model

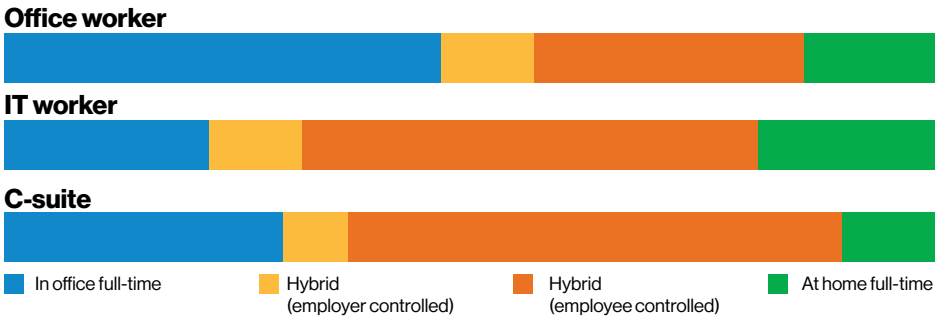


Figure 3: Ivanti[16]

Hybrid working is certainly popular with users. One in five (20%) said they'd be prepared to take a pay cut to continue working from home at least part of the time – and a not insignificant one, the average was 8%.[17]

Almost half (49%) of workers currently working in the office would prefer to follow another model. Almost three-quarters (73%) of them would like a hybrid model.[18]

Current vs preferred working model

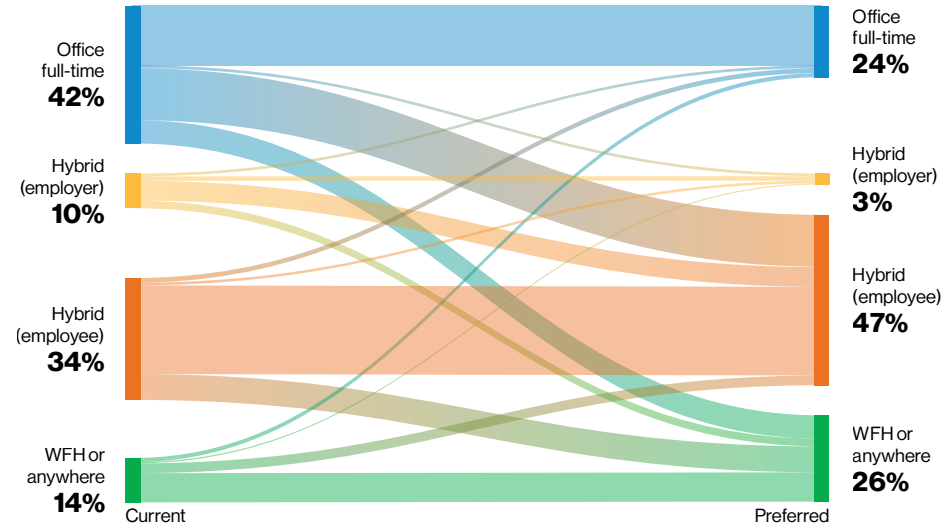


Figure 4: What best describes your current/preferred working arrangement? Ivanti[19]

> **We believe that a structured hybrid approach—meaning employees that live near an office need to be on site two days a week to interact with their teams—is most effective for Zoom. As a company, we are in a better position to use our own technologies, continue to innovate, and support our global customers.**
>
> A Zoom company spokesperson reported in the New York Times[20]

16 Ivanti, Elevating the Future of Everywhere Work, 2023
17 ibid.
18 ibid.
19 ibid.
20 New York Times, Even Zoom Is Making People Return to the Office, 2023

Taking work home or bringing risks to work?

The increase in remote working is not without its downsides. A survey by Fortinet found that 62% of companies had experienced a security compromise that was at least partly attributable to remote working in the past three years.[21]

62% of companies suffered a security breach connected to remote working.

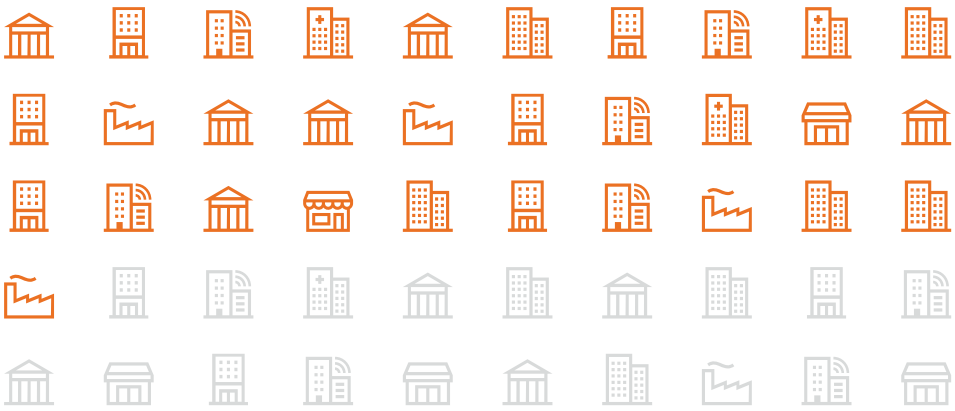


Figure 5: Did you experience a security breach during the past two to three years that could be at least partially attributed to an employee working remotely? Fortinet[22]

The inability to extend corporate security to a non-owned environment means that working from home presents several potential additional risks, including:

- Poorly secured home networks – including unpatched devices, weak encryption and lax password management
- Multiple unknown users and devices – family, friends, housemates, smart home devices, etc.
- Increased use of work devices for personal tasks – including by family members
- Lower policy adherence – users may be less rigorous about following security policies in a non-corporate environment

Ideally, organizations would be able to establish consistent policies across all devices and all locations. Fortinet found that companies are evenly split: 42% use the same vendors across endpoint device types and 42% use different vendors.

An HBR study of remote workers found that, 67% of the participants reported failing to fully adhere to cybersecurity policies at least once, with an average failure-to-comply rate of once out of every 20 job tasks.

Harvard Business Review[23]

See section on home Wi-Fi security on page 22.

21 Fortinet, 2023 Work-from-Anywhere Global Study, 2023
22 ibid.
23 Harvard Business Review, Research: Why Employees Violate Cybersecurity Policies, 2022

Users not as savvy as they think

Proofpoint has been tracking the awareness of cybersecurity among users and has generally seen an upward trend. Users say all the right things: When asked in surveys, they say that they know to be suspicious of unsolicited emails and to be wary of attachments.

Figure 6: Awareness of threats among users. Proofpoint[24]

Yet, the evidence shows otherwise. IBM's X-Force Threat Intelligence Index found that 53.2% of victims clicked on the link in a simulated targeted phishing attack.[25] As we've said before, attackers continue to rely on phishing because it works.

> **Most employees want to be able to work anywhere—in the office when meetings require it, at home (or away) when it benefits them. But delivering on Everywhere Work requires a change of mindset, culture and technology. And securing it will be among the top priorities—and accomplishments—of 2023.**
>
> Ivanti[26]

24 Proofpoint, State of the Phish 2023, 2023
25 IBM, 2022 X-Force Threat Intelligence Index, 2022
26 Ivanti, Elevating the Future of Everywhere Work, 2023

Phishing is still a popular pastime.

The 2023 DBIR reported a doubling of "Social Engineering" incidents, largely due to the use of pretexting – a tactic commonly used in business email compromise (BEC) attacks. Compounding the problem, the median amount stolen in these has increased over the past couple of years, reaching $50,000.[27]

Data from Lookout on the number of unique URLs accessed by users on both consumer and enterprise devices (see Figure 7) shows that the number interacting with more than six malicious links is increasing each year. This is probably due to the increasing sophistication of phishing campaigns and the blurring of the lines between personal and work use on mobile devices.

> **The mobile device presents a fundamentally different environment from a laptop or desktop. These devices can give a significant leg up to attackers who use the smaller screens, simplified interfaces and hidden URLs to their advantage. This, coupled with our natural tendency to immediately tap on anything that comes up on our smartphone or tablet screen, gives phishing attacks a higher chance of success.**
>
> Aaron Cockerill, Executive VP of Products, Lookout

Number of devices on which a phishing link was clicked

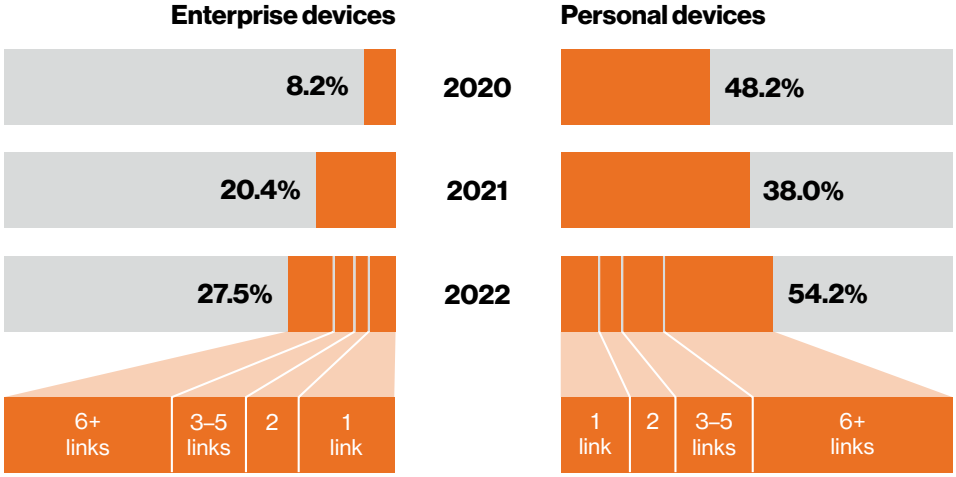


Figure 7: Analysis of users clicking on dangerous links. Lookout[28]

Despite this, nearly two-thirds (65%) of companies still don't perform phishing simulations.[29] And, we'd venture to say, even those that do rarely scope non-email-based variants (such smishing, using SMS messages) into their campaigns.

84%

of organizations experienced at least one successful phishing attack between September 2021 and August 2022.

Proofpoint[30]

80%

of phishing sites target mobile devices specifically or are designed to function both on desktop and mobile. Meanwhile, the average user is 6–10 times more likely to fall for SMS phishing attacks than email-based attacks.

Zimperium[31]

27 Verizon, Data Breach Investigations Report, 2023
28 Lookout, The Global State of Mobile Phishing, 2023
29 Proofpoint, State of the Phish 2023, 2023
30 ibid.
31 Zimperium, 2023 Global Mobile Threat Report, 2023

Everything is going hybrid.

Hybrid cars, hybrid work and now hybrid phishing. Hybrid phishing combines multiple techniques to increase the effectiveness of attacks. This often includes a combination of large-scale, automated tactics and more targeted methods. For example, pairing an email phishing attack with a voice-phishing (vishing) attack.

Telephone-oriented attack delivery (TOAD) is a form of hybrid phishing that emerged in 2021. Since then, the number of instances of this type of attack has been steadily rising. Proofpoint said that it sees up to 600,000 TOAD messages per day.[32] That's a tiny number compared to the total number of phishing messages sent – many individual phishing campaigns send millions of messages. But the higher degree of effectiveness makes this type of attack something to take very seriously.

Adding a vishing element to a click-targeted phishing campaign tripled its effectiveness, eliciting a click from 53.2% of recipients, according to IBM's 2022 X-Force Threat Intelligence Index.[33]

A typical TOAD attack consists of sending a message containing one of the common phishing messages or payloads – such as a fake invoice, an update on an invented delivery or a warning about an account being compromised and the password needing to be reset. What sets it apart from a standard phishing attack is the inclusion of a customer service (or should that be victim service?) number for recipients with questions.

This lends credibility to the attack. It shouldn't.

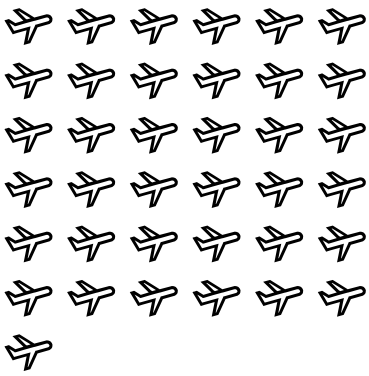
Big exec compromise?

Business email compromise (BEC) attacks, which we covered in detail in the 2022 Mobile Security Index, continue to be one of the most lucrative types of attack for cybercriminals. The Federal Bureau of Investigations (FBI) IC3 unit has reported that Investment and BEC attacks made up over half of the US $10.3 billion in losses reported to it in 2022. The reported losses associated with BEC attacks averaged US $125,611.67 each.[34]

Investment fraud

$3,311,742,206

~37 Boeing 737-700s (sticker price)



Business email compromise

$2,742,354,049

~31 Boeing 737-700s (sticker price)

Figure 8: Reported losses in 2022. Top two categories. FBI[35]

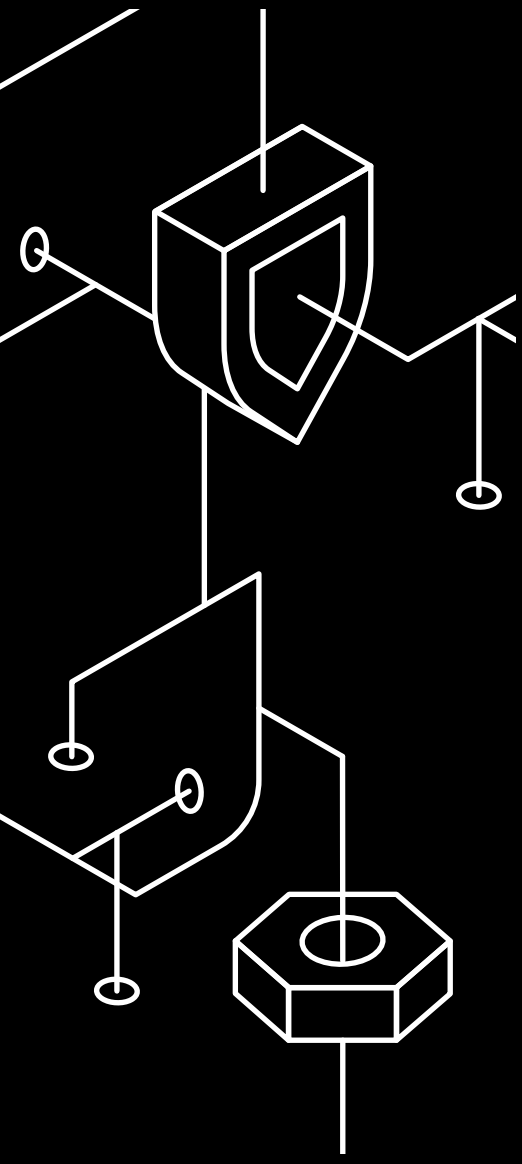
Don't believe your eyes or ears.

The recent growth of generative artificial intelligence (GAI) has shown that we can no longer believe our eyes. Anybody with internet access can create a deep fake image or video. Attackers are exploiting this technology to make phishing attacks even more effective.

Researchers have found that seven words can be enough of a sample to create a believable impersonation of an individual's voice. That YouTube interview with the CEO could very easily be turned into a convincing voicemail instructing an employee to change the payment details of a large supplier or reset credentials to an important system.

32 Proofpoint, State of the Phish 2023, 2023
33 IBM, 2022 X-Force Threat Intelligence Index, 2022
34 FBI, Internet Crime Report 2022, 2022
35 ibid.

Balancing security and user experience



The COVID-19 crisis forced many companies to adapt quickly. They generally did a pretty good job of adjusting to the new reality, including enabling remote work. But now they're thinking about the future, how to secure the business, and how to support users in a sustainable and flexible way.

As remote working increases and workloads shift to the cloud, many are turning to approaches based on zero trust and secure access service edge (SASE). These approaches are designed for the hybrid-working, cloud-first, mobile-first and perimeter-less world of today – and tomorrow.

The traditional way to secure remote workers was to use a virtual private network (VPN). Once established, a VPN connection is trusted implicitly. With this model, potentially thousands of devices, applications and users could have wide-ranging access to the organization's network and sensitive data. It was also not a very user-friendly experience.

If employees can't easily access the applications and systems they need to do their work, they may not be as productive. It's a delicate balance, but you can deliver a frictionless remote work experience while also helping to keep the organization secure.

A zero-trust approach can help strengthen a company's security policy and make it more resilient. It can also improve the user's experience. For example, intelligent, analytics-driven identity access management solutions can automate the process of determining when to grant a specific user access to certain applications. AI-driven threat detection solutions can also help the organization detect anomalies, suspicious user behavior and network activity, and isolate these threats before a breach occurs.

With this approach, employees:

- Don't have to deal with onerous authentication requirements
- Aren't unintentionally blocked from systems they need to do their jobs
- Aren't given unauthorized access to sensitive data

A zero-trust model can also help give employees the flexibility they want. With an approach focused on verification rather than implicit trust, companies can deliver a better employee experience and remain agile in the increasingly complex threat environment.

Zero trust is one of the foundational components of the SASE framework.

While the promise of digital transformation remains a priority, the reality for most enterprise technology teams is that managing and securing an increasingly complex IT environment poses major challenges. This paper explores how SASE can help secure and optimize your unique network environment.

Read more ›

Applications

Malware

Before you skip ahead, thinking you've got this one in hand, pause for a minute to consider that nearly 1 in 10 (9%) organizations were hit by mobile malware in 2022.[36]

Check Point identified a "vast increase in the number of malicious applications infiltrating Google and Apple stores." One approach is to create a simple app – like an "improved flashlight" or a puzzle to make that long journey less boring – with malware baked in. Apps like this raise few red flags in people's minds – "It's only a flashlight, what harm can it cause?" But many attackers now hide their malicious code in modified versions of legitimate apps.

These malicious variants (MVs) can appeal to users for several reasons. Who hasn't searched for an app to perform a one-off task, then edited the search to include the word "free?" Attackers often tempt users with a free trial or extended functionality not available in the legitimate free version. This isn't just about games with extra lives or other frivolous things. Attackers have released modified versions of apps like OpenVPN and SoftVPN.

App updates that take away popular features – as some social platforms have done recently – are a boon for attackers. Users can be tempted with the promise to revert to a version with the functionality they miss. The modified app doesn't even have to deliver, just get the user to try it.

One of the weaknesses with apps is that it's quite difficult to tell what data they are sending and how securely. Awareness of threats has grown over the years. For example, many users know to look out for the padlock when visiting a website. They may not know exactly what it means, but they know it's important. However, when using an app, there's no reliable visible indicator that data is encrypted in transit.

+30%

Mobile app threats increased by over 30% between the first half of 2022 and the first half of 2023.

Lookout[37]

40%

Malware showed up in 40% of breaches.

Verizon 2023 DBIR[38]

36 Check Point, 2023 Cyber Security Report, 2023
37 Lookout, Lookout Security Graph, 2023
38 Verizon, 2023 Data breach Investigations Report, 2023

Ransomware

Over the past few years, ransomware has risen faster than a K-pop band. It can take many forms: crypto ransomware, lockers, scareware and doxware. As awareness has grown, so has preparedness. But the attacks keep happening, and many companies are affected.

Some may be under the illusion larger enterprises are a more attractive target as they present a higher potential payoff, but an Akamai analysis of victims by revenue paints a different picture.[39] More than 60% of victims have annual revenue under $50 million per year – but obviously, there are more organizations of this size. Organizations with revenue of over $1 billion make up only 0.03% of the total population, but over 8% of the victims.

24.7%

Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24% of breaches.

Verizon 2023 DBIR[42]

Victims of ransomware by revenue band

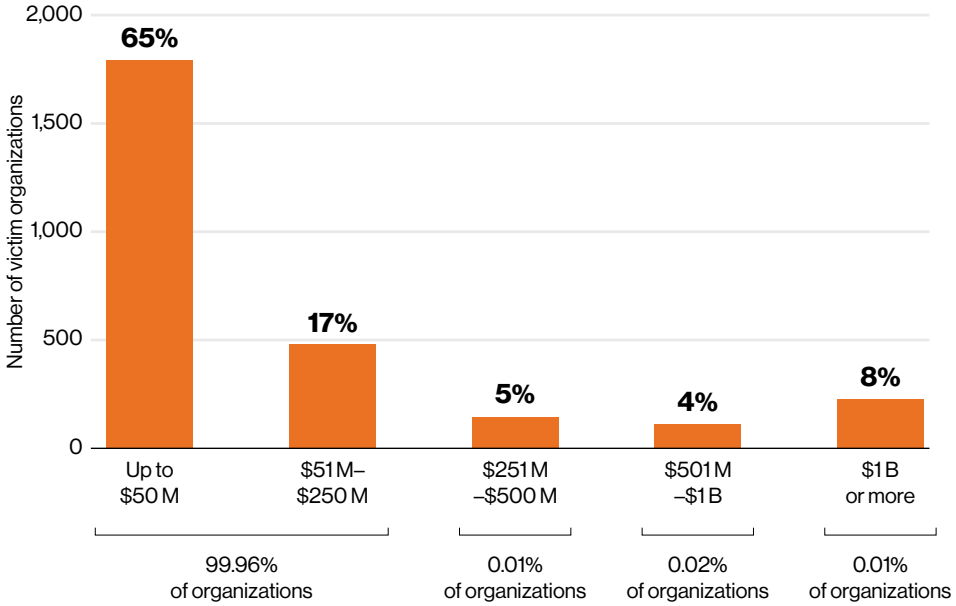
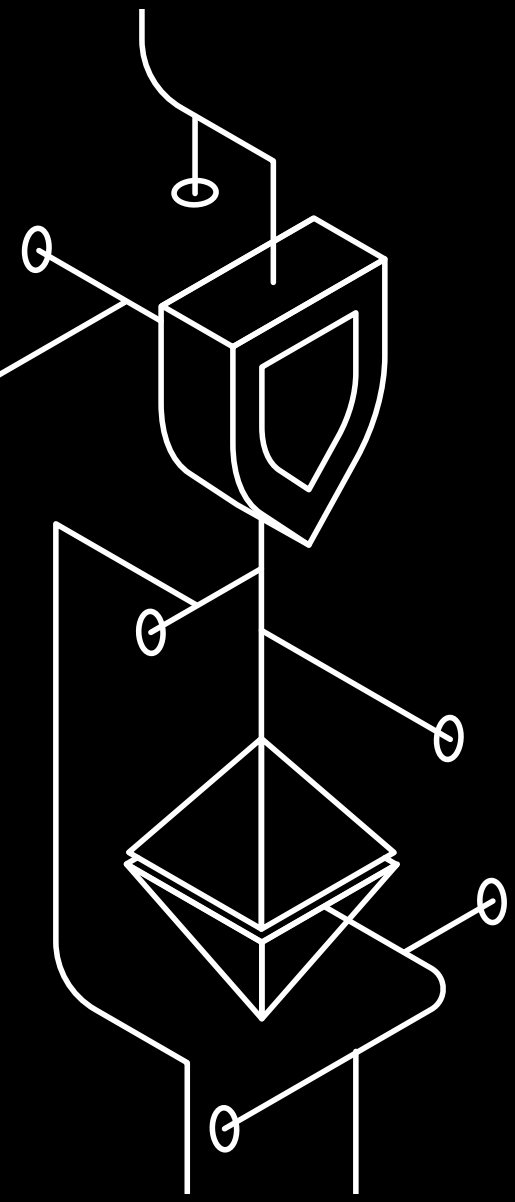


Figure 9: Number of companies falling victim to a ransomware attack by company size. Data from October 1, 2021 to May 31, 2023. Akamai[40]

IBM's 2023 Cost of a Data Breach report found that despite ongoing efforts by law enforcement to collaborate with ransomware victims, 37% of respondents opted not to bring them in. Nearly half (47%) of studied victims paid the ransom.[41]

39 Akamai, Ransomware on the Move, 2023
40 ibid
41 IBM, Cost of a Data Breach Report 2023, 2023
42 Verizon, 2023 Data Breach Investigations Report, 2023

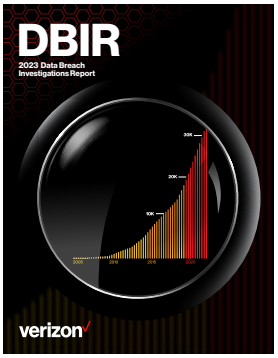
Balancing security and freedom



In an era where innovation and flexibility are vital for success, restricting employees' digital actions can be problematic. Be too strict and you can alienate employees, stifle creativity and impede productivity. But with cyber threats high on the corporate agenda, robust security is essential.

To find the right balance, it's important to cultivate a security-aware culture. Regular training sessions can educate employees on the importance of security measures, turning them into proactive defenders rather than potential vulnerabilities. Leveraging tools like zero-trust frameworks, which prioritize continuous verification over perimeter defense, can also help ensure security without unnecessarily hindering employees.

Furthermore, adopting user-friendly security solutions can make compliance less burdensome. For example, modern MFA methods can be both secure and seamless. Lastly, maintaining open lines of communication between IT departments and other employees can help tailor security policies that protect without getting in the way – too much.



Verizon Data Breach Investigations Report (DBIR)

The DBIR provides security professionals with an in-depth, data-driven analysis of real-world instances of cybercrime and how cyberattacks play out across organizations.

Each year, our DBIR team analyzes tens of thousands of incidents and breaches from around the world. They identify cybersecurity trends and help organizations take a data-driven approach to optimizing their cybersecurity programs.

The analysis covers incidents recorded by organizations from different verticals and disparate geographic locations. This includes small and medium businesses (SMBs), enterprises and public-sector organizations.

Reading the DBIR can help you to understand the particular threats your organization is most likely to face and help prepare you to handle them in the best possible manner.

Read more >

Devices and things

BYOD

The vast majority of organizations with a bring-your-own-device (BYOD) program give employees a stipend. A study by Oxford Economics and Samsung found that this is generally in the region of $30 per month to $50 per month.

"While BYOD companies do not pay for the employee device or service plan, the vast majority (98%) do pay a monthly stipend to employees to compensate them for the use of their personal mobile device. The average mobile stipend per month across our survey is $40.20, or $482 per year per employee."[43]

Alternative device ownership/control models, such as those shown below, may enable companies to offer employees more freedom, with fewer security and administration headaches.

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

Figure 10: Device ownership and management models.

50%+

In 2022, more than 50% of personal devices were exposed to a mobile phishing attack.

Lookout[44]

$482

Average annual stipend for employees on company BYOD program.[45]

"BYOD companies also indicate that the cost of administering the stipend is a significant part of their management costs.[46]

43 Oxford Economics and Samsung, Maximizing Mobile Value 2022, 2022
44 Lookout Security Graph Data, January 1st–December 31st, 2022
45 Oxford Economics and Samsung, Maximizing Mobile Value 2022, 2022
46 ibid.

Device loss/theft

According to the 2023 Verizon DBIR, the loss of devices continues to dramatically outweigh theft. This is contrary to the picture across all breach types, where 83% involved an external actor. Theft hit a high point compared to loss during the COVID-19 period, but remained at under 10% of Lost and Stolen Assets breaches.[47]

Loss and Theft incidents

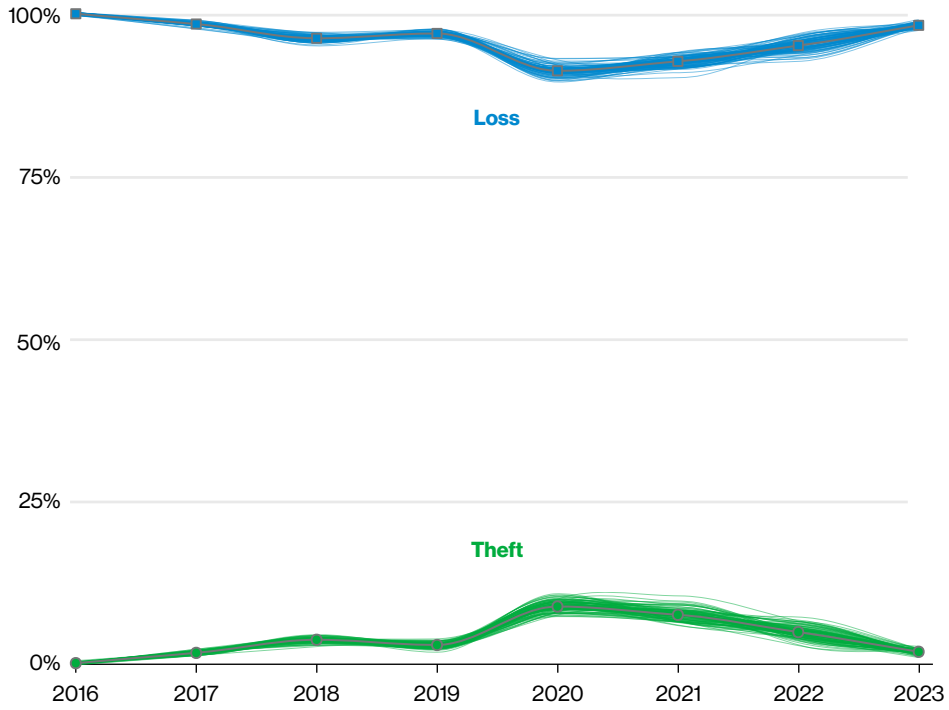


Figure 11: Top Action varieties in Lost and Stolen Assets incidents. Verizon[48]

Less than 10% of the Lost and Stolen Assets incidents analyzed as part of this year's DBIR were confirmed data breaches. This is largely because the status of confidentiality disclosure remains "at-risk" rather than "confirmed." Even if a device has been stolen, that's not to say that the thief was after the data. Whether found or stolen, the recipient may be more interested in the hardware.

As we stated in the 2022 MSI, loss and theft isn't something most companies are that concerned about. This is largely because it's relatively easy to mitigate against.

Four of the Center for Internet Security (CIS) Critical Security Controls are key:

3.	**Data protection**
6.	Encrypt data on end-user devices
9.	Encrypt data on removable media
4.	**Secure configuration of enterprise assets/software**
10.	Enforce automatic device lockout on portable end-user devices
11.	Enforce remote wipe capability on portable end-user devices

SIM theft

SIM theft, not to be confused with SIM swapping, is the robbery of a SIM card with the intent to use it for unauthorized calls or data. While relatively rare, as the number of connected devices grows and there are more SIMs in devices in remote and insecure locations, this could become more of a problem.

Putting policies in place to quickly block any SIMs that might be compromised can help mitigate the potential losses.

According to the Federal Communications Commission (FCC), eSIMs offer significant security benefits because they can't be stolen without stealing the devices themselves.[49] That might not make a lot of difference if the device is a phone, but many connected devices – such as smart streetlights and connected earthmovers – are more difficult to steal.

For devices with physical SIMs, some operators offer services that bind a SIM to a single device (using the IMEI number). This makes SIM theft practically impossible.

47 Verizon, Data Breach Investigations Report, 2023
48 ibid.
49 Federal Communications Commission, eSIM Cards FAQ, 2023

Internet of Insecure Things?

There are billions of connected things. And the rate at which that number is growing is set to increase with the realization of 5G—just do a search for "mass IoT."

Securing IoT devices is one of the most challenging aspects of mobile device security. Attacks targeting IoT devices are rapidly evolving as:

The number of devices grows

Making the devices an appealing target as an attack vector.

The power of devices increases

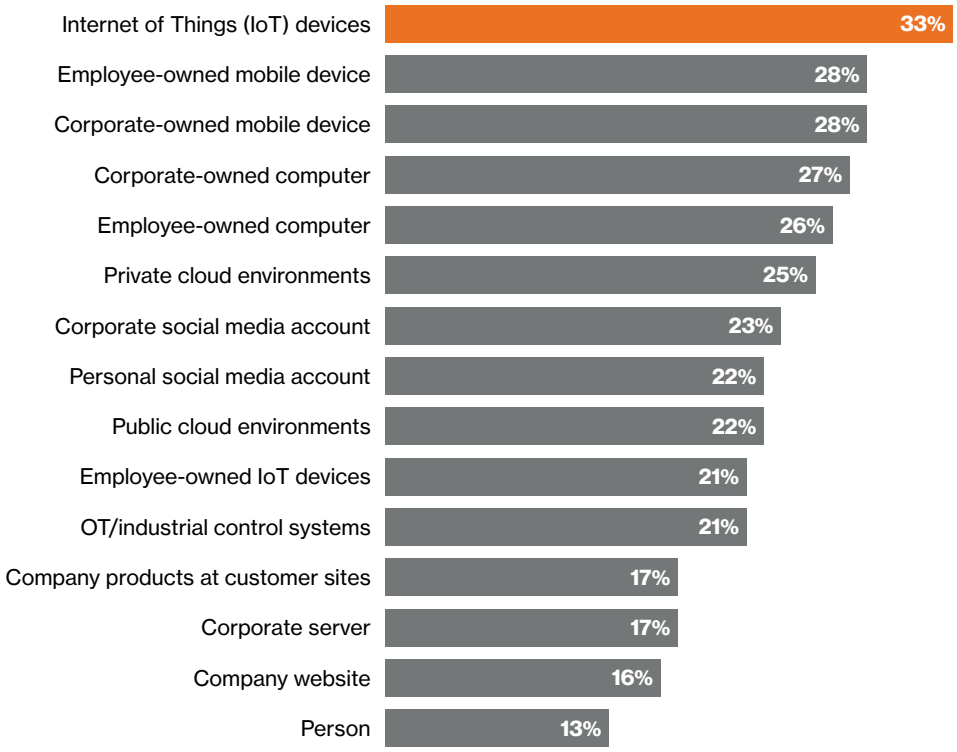
Making them a potential vehicle for attacks, such as part of a botnet used to carry out a distributed denial-of-service (DDoS) attack.

The applications become more mission-critical

Making the devices themselves targets.

One of the challenges of securing IoT devices is that many organizations don't have centralized coordination of projects. IoT projects are often led by the lines of business and don't even have to follow standard security requirements.

Most common targets

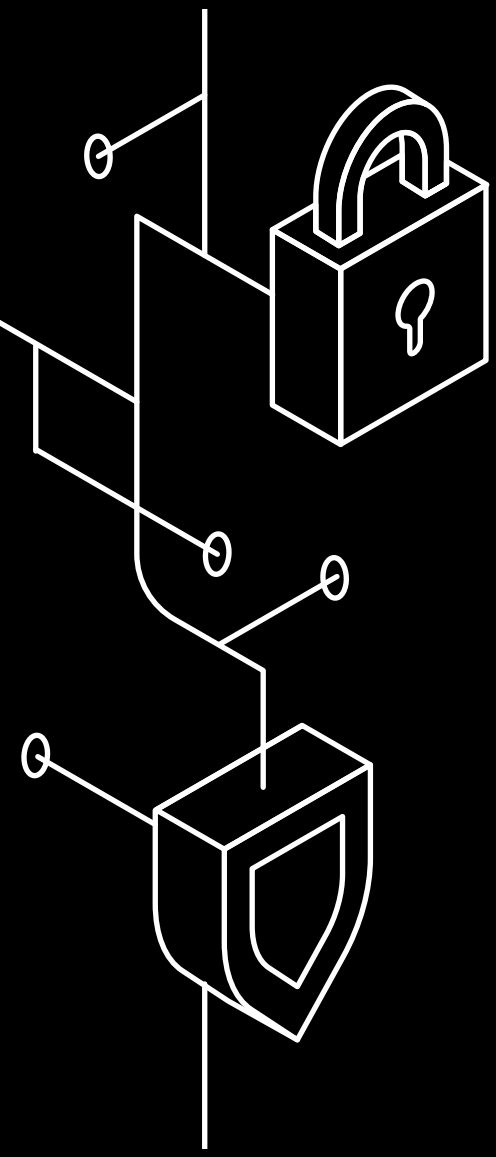


A 2022 Forrester study found that IoT devices were the most commonly reported targets of external attacks.[51]

Figure 12: Forrester[50]

50 Forrester, The State Of IoT Security, 2023
51 ibid.

Balancing security and privacy



Whether a company operates a BYOD policy or not, there's an inherent conflict between work and personal use.

Half (50%) of users checked personal email/messaging apps on their work device(s). Almost as many (48%) let a friend or family member use the device.[52] This blurring of lines could pose a significant security risk.

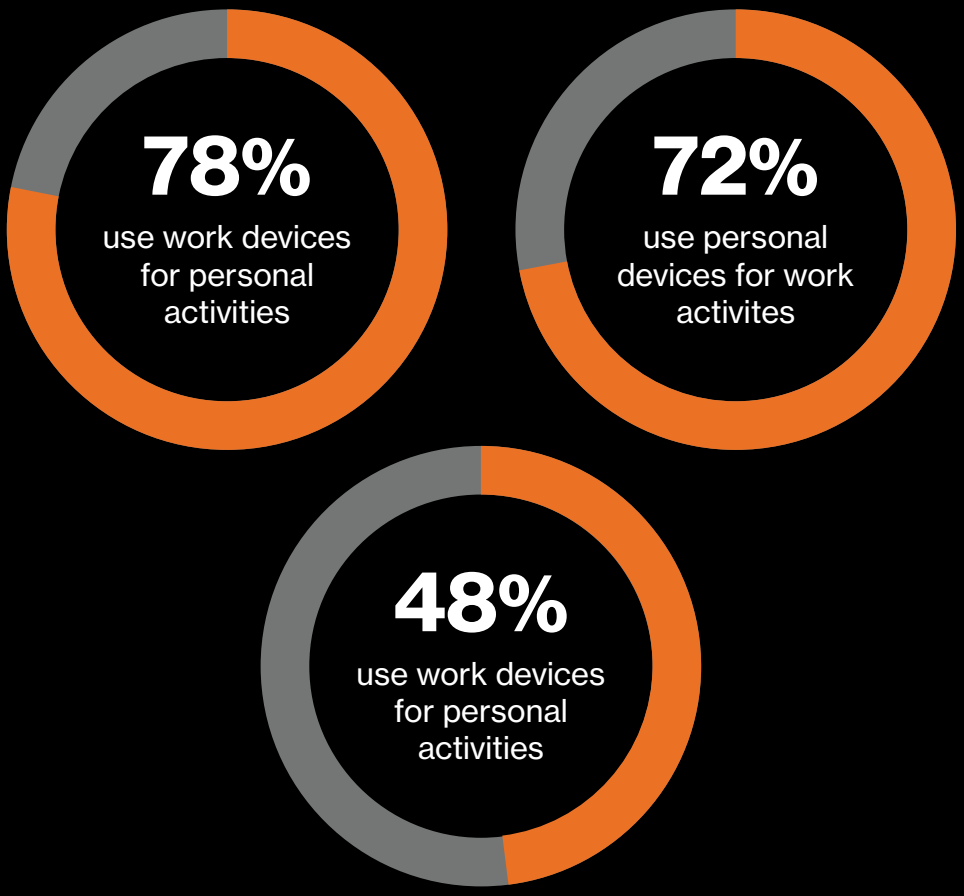


Figure 13: Work/personal device usage. Proofpoint[53]

People often store all kinds of personal information on their devices. This includes photos, messages, emails, contacts and location information. Even just which apps a user has installed on the device could reveal information about their personal life that they'd rather not share – Flo user? Candy Crush addict?[54]

Even if work and personal personas are separated on the device, there can still be dangers. Take location data as an example. Information about where a person is and when could be a privacy violation.

52 Proofpoint, State of the Phish 2023, 2023
53 ibid.
54 Seriously, still?

Networks and clouds

Home Wi-Fi

A staggering 71% of users don't change the default password on their home Wi-Fi. Nearly a third (31%) don't password-protect their home Wi-Fi at all.[55] This is actually an improvement, year over year. At this rate, by 2054, all users will take these basic security measures. That's a long time to wait.

Measures taken to secure home Wi-Fi

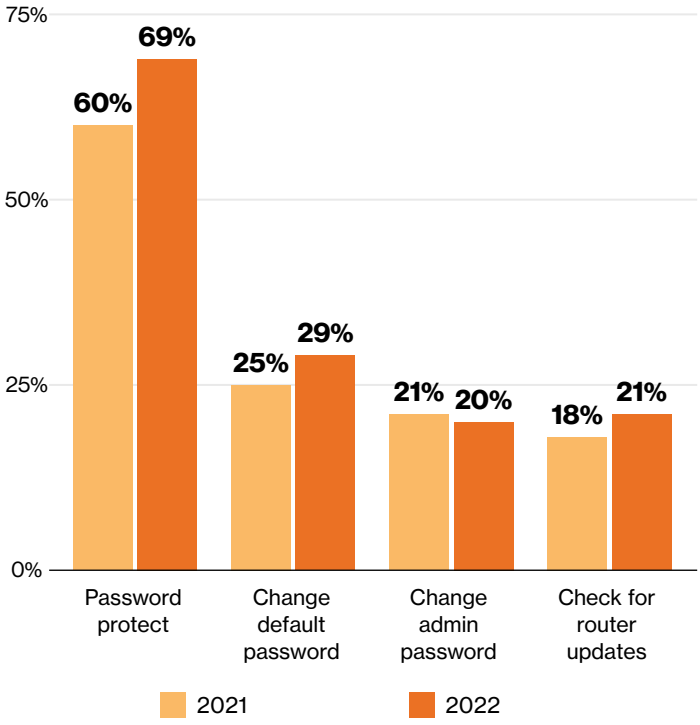


Figure 14: Measures taken to protect home Wi-Fi.[56]

Additionally, 7% of users don't take any measures to protect their home Wi-Fi. That's worrying with the elevated number of users working from home.

Public Wi-Fi

The vast majority (90%) of remote workers access corporate resources from locations other than their home – the average is five different locations.[57] This can expose the organization to additional security risks.

According to a study published in Forbes, 40% of respondents had had their information compromised while using public Wi-Fi.[58]

Clouds

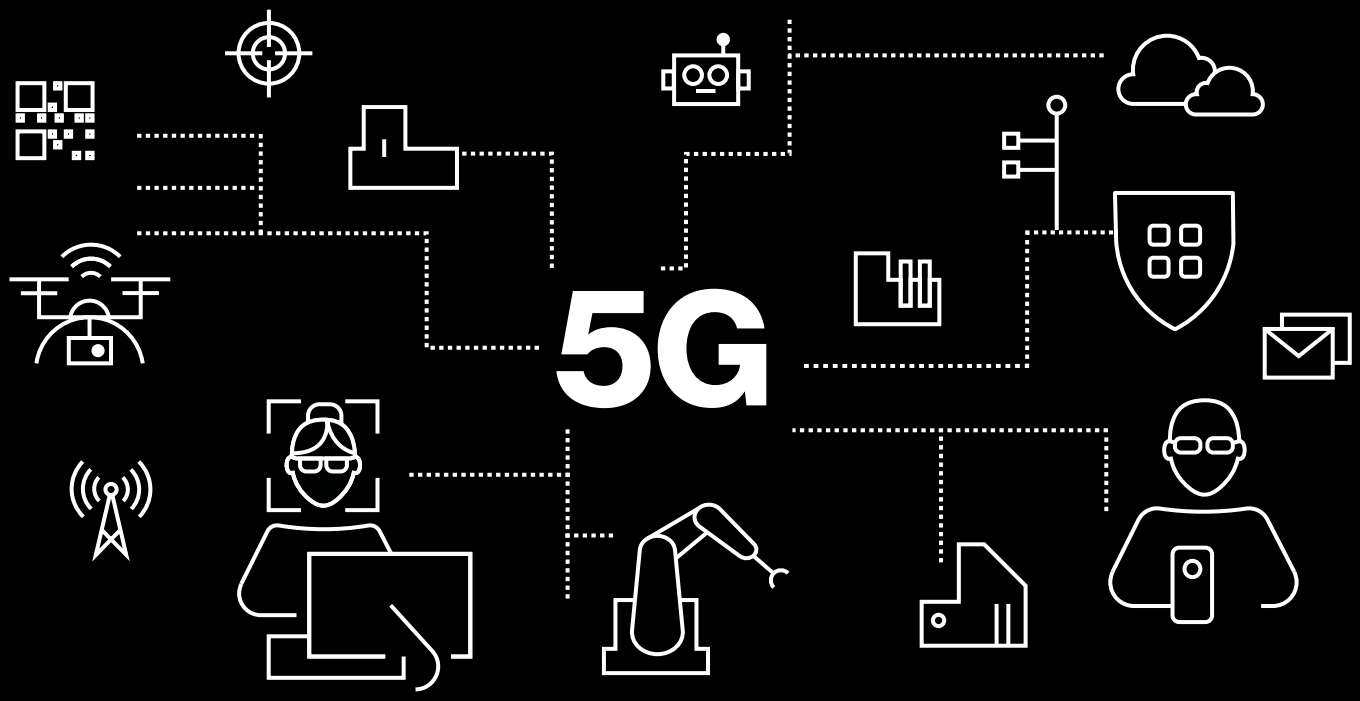
It's widely accepted that organizations are embracing the cloud and its many benefits. We see it all the time. Companies want to move to network models like Network as a Service and SASE that are designed for more cloud-centric architectures. Security is often cited as a limiting factor – 43% believe that the risks are more significant when using the public cloud versus an on-premises environment.[59] Arguably, the cloud isn't less secure; it just requires different tools and approaches. A key reason why data and systems are at risk is actually that they are now available outside the physical perimeter of the organization.

39% of respondents have more than half of their workloads in the cloud. 58% plan to reach this level in the next 12–18 months.

Fortinet[60]

Mobile devices can offer an appealing target as an entry point to critical business for all the reasons stated earlier. That helps to explain why a quarter (25%) of organizations named securing access from personal and mobile devices as one of their biggest operational headaches in securing cloud services.[61]

55 Proofpoint, State of the Phish 2023, 2023
56 ibid.
57 Lookout, The State of Remote Work Security, 2023
58 Forbes, Forbes Advisor: The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data, 2023
59 Fortinet, 2023 Cloud Security Report, 2023
60 Fortinet, 2023 Work-from-Anywhere Global Study, 2023
61 Fortinet, 2023 Cloud Security Report, 2023



5G

With speeds measured in gigabits per second, single-millisecond latency and unlimited data plans, 5G is poised to disrupt how users – consumers and businesses – use mobile devices.

You've probably read all that before. But alongside cutting-edge solutions – such as mass IoT, real-time video analytics and remote surgery – 5G is likely to drive changes that affect even the mundane parts of our everyday lives.

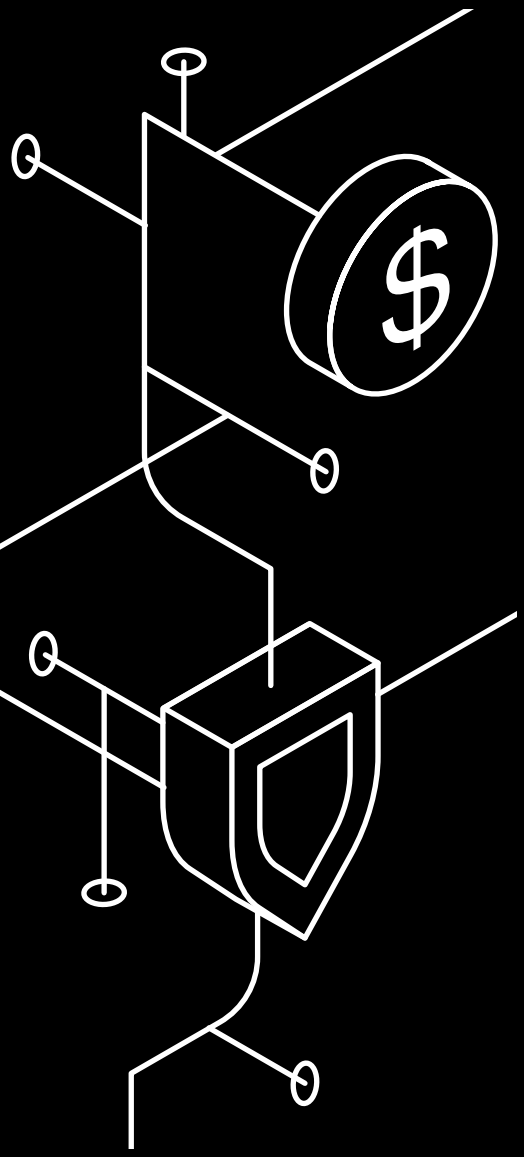
Today, it's the norm to wait until you get home or into the office to download a large file, application or OS update. But with 5G download speeds close to – or even faster than – typical broadband speeds, users might start to question why they should wait.

For example, the next time those users experience patchy performance on a video call – because the kids are gaming upstairs or it's early evening and all the neighbors are binging the latest Netflix must-watch show – they might ask themselves why they need to connect their work devices to their home Wi-Fi at all.

> **"The question is why a consumer would choose to connect their 5G unlimited-data mobile device, via their home router, to a fixed network (where on average, over 25 different devices such as laptops, tablets, IoT devices, etc., are sharing the fixed network resources).**
>
> Vikram Singh, Allot[62]

62 Allot, 5G Adoption and the Role of Network Native Security, 2023

Balancing security and cost



There's always a balance to be found between security and cost. New options could change the dynamics and redefine the value equation.

Connected laptops

One approach would be to switch to connected laptops. According to Dell, the demand for connected laptops "has been steadily increasing over time, due the rise in hybrid (onsite and offsite) or remote work environments and in road warrior style occupations."[63] A laptop with a built-in SIM could give users a better experience and help improve security. With widespread high-bandwidth LTE and 5G coverage, the need to use unknown Wi-Fi should be greatly reduced.

Fixed wireless access (FWA)

It may sound like an oxymoron, but FWA could help secure home workers and small sites. FWA can offer broadband-like performance without the need for physical cabling and disruption. Options range from dongles designed to support one or a few devices to routers that can support dozens of devices.

Giving employees a company owned LTE or 5G broadband solution at home would certainly be more expensive than just expecting a free-ride on their home Wi-Fi, but could it make business sense? Here are three reasons why.

More secure?	As a company-owned asset, the company will have full control of its use. The company could block unknown devices, prevent certain types of traffic (e.g., gaming) and enforce policy updates – all things that would be nearly impossible to achieve or extremely unpopular on the employee's home Wi-Fi.
More reliable?	Aside from the issue of neighborhood contention, there can be competition for bandwidth within the home. There can be dozens of devices connected to the router: phones, laptops, tablets, gaming consoles, TVs, security systems, lights and heating. It's not uncommon to have more than one person working or studying from home. With all those devices, it's not uncommon to suffer performance issues. How does that affect productivity and the employee experience?
Less admin?	Some companies pay their employees a stipend or allow them to claim some work-from-home costs on expenses. Could it be more efficient to provide them with a broadband account? LinkedIn is full of photos of people with a new job and the swag that they've received from their new company. An employee perk that includes a work router could make an employer look really considerate. Who said that being security conscious can't also be an employee benefit?

An FWA connection dedicated for work could help give home workers a reliable level of performance and avoid contention with other members of the household. Because there wouldn't be any conflict between personal and private, the company would be free to implement updates and security policies to protect the user and corporate assets.

63 Dell, A Guide to Understanding 4G/5G Connected Laptops, 2023

Conclusion

As businesses have evolved, mobile devices have become indispensable tools. They serve as vital entry points to a company's key systems, data and cloud-based resources. They can also put these resources at risk.

Mobile devices offer vast improvements in productivity and flexibility, but they also introduce a myriad of security challenges. Striking a balance between robust security, productivity and cost isn't easy. And organizations also need to factor in user experience and privacy too.

Overburdening users with intrusive security measures can deter productivity. But lax security protocols would expose critical company systems and assets to threats. Getting this balance right is a career-determining, future-deciding, board-level issue.

Effectively protecting mobile devices and preventing them becoming the organization's Achilles heel entails leveraging solutions that provide robust security while ensuring seamless user experience. Investing in continuous employee training, adopting multi-layered security protocols and using scalable, cloud-native solutions can help in achieving this delicate balance.

The future of business is undeniably mobile, but it's imperative that we don't sacrifice security. Ensuring that our mobile devices are both secure and functional should be a top priority for every forward-thinking organization.

93%

of organizations said that their board of directors has asked about the company's cyber defenses and strategy.

Fortinet[64]

64 Fortinet, 2023 Security Awareness and Training Global Research Brief, 2023

Contributors

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's being done to mitigate them. This white paper wouldn't have been possible without the data and insight provided by Akamai, Allot, Check Point, Fortinet, IBM, Ivanti, Lookout and Proofpoint.

Check Point leading cyber security solutions protect corporate enterprises and governments globally. Its portfolio protects all organizations from cyber-attacks with an industry leading catch rate of malware, ransomware, and other threats. Harmony, for remote users; CloudGuard, to secure clouds; and Quantum, to protect perimeters and datacenters. Check Point protects over 100,000 organizations.

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver excellent digital employee experiences and improve IT and security team productivity and efficiency.

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver and secure their digital experiences – helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away.

FortiGuard Labs is Fortinet's cybersecurity threat research organization, comprised of the industry's most knowledgeable threat hunters, researchers, analysts, engineers, and data scientists. It provides industry-leading threat intelligence and security services, contributing significant resources to foster sharing actionable threat intelligence across public and private partners to disrupt cybercrime globally.

We're the data-centric cloud security company that reduces risk and protects data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards corporate data across devices, apps, networks and clouds and is as adaptive and simple as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to connect freely and safely.

Allot is a leading provider of innovative network intelligence and security solutions that empower communications service providers (CSPs) and enterprises worldwide to enhance the value they bring to their customers. With over 20 years of proven success, our solutions turn network, application, usage and security data into actionable intelligence that make our customers' networks smarter and their users more secure.

IBM Security MaaS360 transforms securing smartphones, tablets, laptops, desktops, wearables and IoT without sacrificing a great user experience. 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.

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, we help 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.

About the cover

The cover illustrates the idea of balance, the theme of this year's report. The organization must put numerous security measures in place to protect data and systems from attack, but it must also consider cost, freedom, privacy and control. Put too much burden on users and you could affect productivity, motivation and introduce security fatigue – which could actually make the organization more susceptible to threats. Give up to much control and you could expose the organization's most valuable assets, its crown jewels, to greater risk. The picture shows that this is a delicate balance to achieve. You might think that you've found it, but without the right insight, strategy, policies and tools it could be fleeting.

verizon