Securing 5G's future

Why cybersecurity is key to realising the full promise of 5G networks

Contents

Executive summary

Combining opportunity and security in the 5G world

Across the world, connected devices are changing how people live and work. The communications networks that link these devices and enable them to talk to one another are integral to this evolution. In this context, the roll-out of faster, higher-bandwidth 5G networks is a significant step forward — but one that also needs to be kept in perspective. Despite the hype surrounding 5G, the reality is that many of the services that it will enable have already been provided through its 4G predecessor and various low-power wide-area networks (LPWAN).

That said, the technology underlying 5G marks a break with the past in some important ways, including a fundamental reconceptualisation of what a communications network looks like. The previous four generations of mobile technology were founded on physical architecture. Although 5G includes new hardware, it is first and foremost a virtual network — finally turning the convergence of networks and wireless communication into reality. This breakthrough will unleash a wave of innovation, but the greatest impact will perhaps be felt through new or enhanced uses of wireless technology. These may include Fourth Industrial Revolution (4IR) infrastructures, smart cities, autonomous vehicles, remote surgery and new, more powerful artificial intelligence (AI) systems.

Today, this is happening against the backdrop of the COVID-19 global health emergency. Because many governments have enacted various stay-at-home orders, larger numbers of people will be working from home via communications links that are increasingly based on 5G networks. Companies that are more advanced in their digital transformation are telling us that their investment in technology, cybersecurity and resilience has paid off as they respond to the novel coronavirus.

But these shifts have also placed intense scrutiny on cybersecurity. Some commentators have suggested that 5G networks increase the potential attack surface for cyber adversaries, because 5G connects many more devices than previous technologies and uses distributed processing power ‘at the edge.’ However, many of 5G’s anticipated vulnerabilities result from other elements of the 5G ecosystem — notably the security of the end devices. The good news is that the challenges to cybersecurity in 5G networks can be overcome, providing a solid basis for innovation by parties worldwide to deliver the full promise of this technology.

Entering the 5G era

We are on the threshold of a world supported and connected by 5G-enabled massive Internet of Things (mIoT) capabilities. In this world, 5G helps to provide the bedrock for our smart cities, our 4IR operating models, our smart homes, our smart transportation, our smart healthcare and myriad other potential use cases. PwC's recent paper *The Impact of 5G: Creating New Value across Industries and Society,* published in conjunction with the World Economic Forum, articulates the wide range of existing 5G use cases that are already transforming the business environment.

As with any new technology, the introduction of 5G requires us to revisit our approach to cybersecurity. However, this need should not distract the organisations, governments, cities and industries planning for the 5G revolution from the significant opportunities it offers. In fact, by understanding and countering the risks specific to 5G, companies can build greater resilience, and use 5G as a powerful force to generate revenues and profit in their businesses and good in society. This has become even more imperative today, as the coronavirus pandemic changes how people live and work in unprecedented ways.

When it comes to why 5G is different, the numbers speak for themselves. In combination, its technical attributes — as summarised in "The technical attributes of 5G," on page 5 — mean 5G is capable of achieving speeds approximately 100 times faster than 4G and handling significantly more connections. These advantages are amplified by ultra-low latency — the time it takes to receive a response to a request.

Although consumers are excited by the prospect of downloading ultra-high-definition (UHD) movies in seconds, the true benefits of these technical attributes will manifest themselves through a wide range of innovative applications. These may well change not only how we entertain ourselves but also how and where we work, how we move around, and how we keep ourselves healthy — with AI-enabled personalisation embedded in 5G applications playing a growing role in helping us do these and other things.

The ability of 5G to deliver on its promise is rooted in its being a software-enabled network that's operated through distributed digital routers and optimises processing speed and power by relocating operations to the fringe. This contrasts with the 'hub and spoke' configuration of previous generations of mobile technology.

The ‘zero trust’ approach

Keeping 5G networks secure will be key to realising the full potential benefits for consumers, businesses and entire societies alike, and for ensuring the safety of end users. This has become all the more critical during the coronavirus pandemic, as more and more companies adopt remote working policies and as telemedicine use increases. For example, with staff working outside the office, companies’ IT infrastructure systems are being stretched, creating heightened vulnerability to cybersecurity attacks. And as patients connect with medical professionals via their tablets, laptops or mobile phones, sensitive information will need to remain secure.

A vital first step towards protecting any network against cyber threats — 5G included — is to understand where vulnerabilities might arise. This is primarily at the points of interconnection, where risks transition from one element of the network to another. With 5G, as with 4G, different companies are often involved on each side of these transitions, meaning a coordinated approach is vital to ensure security is effective from end to end. The approach also needs to be agile, given that technology tools are advancing rapidly, and both companies and cybercriminals seek to use them to their advantage.

All participants in the 5G ecosystem — including mobile operators, network vendors, system integrators and end businesses — should agree to identify, profile and assess the health of every component before it’s permitted to connect to the network, and, if appropriate, limit access to the 5G service based on this assessment. This can be achieved with a strategy grounded in the following elements:

1. **Zero-trust approach.** A robust security posture from end to end, for all devices and software, will help reduce risk exposure across the 5G ecosystem. Having been assessed for their level of security before connecting to the network or resources, devices should only be allowed access to resources

The technical attributes of 5G

5G brings significant changes to many aspects of the network — including core and management systems, as well as all protocol layers ranging from radio to applications. Its technical attributes include:

- **Network slicing,** which provides a way for service providers to enable network-as-a-service (NaaS) to specific subscriber groups, giving them the flexibility to manage their own devices and services according to specific needs
- **Enhanced mobile broadband (1–20 Gbps),** which supports applications such as 3D video transmissions with 4K or 8K resolution screens, online gaming and so on
- **Ultra-low latency (<1ms),** which is important for mission-critical services such as augmented reality (AR) and virtual reality (VR), telemedicine and healthcare, intelligent transportation, and industry automation
- **Massive device connectivity** for vehicles, mobile subscribers, enterprises, IoT and the like
- **High availability and dense coverage,** which will make it capable of providing unlimited connectivity for billions of different subscribers
- **Low energy consumption,** with up to ten-year battery life for M2M (machine-to-machine) communications.

To deliver these capabilities, 5G is equipped with a new air interface that supports heterogeneous access networks and handles variable bandwidths. Packet core network upgrades are also being implemented, where traditional and 5G mobile services share infrastructure, to improve service delivery and operational efficiency.

based on their need and security 'health.' Also, all software provisioning — from the core to the IoT device, and from firmware to the cloud — must be treated with a degree of scepticism, with resource hubs verified and code bases checked for malware prior to builds and deployments. Application programming interfaces (APIs) should be segmented and access controlled based on level of risk.

2. Universal encryption. To minimise the risk of data being compromised or corrupted, telecoms operators and other 5G participants should leverage strong encryption methods for securing the traffic between endpoints and services. This involves applying flexible methodologies that allow the encryption to be strengthened progressively over time as standards and risks evolve. Centralised key management processes will help mitigate 'man-in-the-middle' attacks, in which an attacker intervenes in a communication between two parties who believe they're communicating directly with each other.

3. Orchestration by AI. Machine learning (ML) and AI will have a vital role to play in identifying and mitigating ever-changing risks, providing the speed and accuracy of insight and intelligence needed to manage security policy across hyper-dense machine type communications and ultra-low latency applications. The capabilities of AI and ML technologies will see them used throughout the 5G architecture for security orchestration, including such activities as traffic analysis, deep packet inspection (DPI), threat identification and infection isolation.

AI: A powerful tool at the core of 5G networks, applications and devices

As telecoms operators embark on their 5G implementations, they are having to face up to unprecedented network complexity. The key elements driving this network complexity include the high-density distribution of 5G networks, the challenging configurations of large-scale antenna arrays, and infrastructure upgrades required across the network. Telcos will also need to prepare for the ongoing development of solutions to various needs — both predicted and unpredicted — that will emerge from IoT and related smart systems. This will demand an increasingly agile and responsive approach to network management.

AI will be critical in meeting these challenges by facilitating dynamic engagement with network quality, detecting and correcting network issues faster than is currently possible. AI will also be necessary for the full promise of network slicing to be realised; AI will enable operators to optimise their slicing strategies, responsively assessing, evaluating and determining slice allocations.

Looking beyond the network, recent PwC thought leadership has highlighted how the combination of AI and 5G will enable a new wave of connected devices that will redefine the word *smart* in two key respects. First, their user interfaces will be based not only on touch but increasingly also on voice working side-by-side with touch or even without it. Second, they will use discrete apps to trigger specific tasks requested by users and apply AI-driven algorithms to anticipate users' needs and meet them proactively.

Through these advances, AI and 5G will deliver a number of impacts for end users. One will be greater personalisation, as data transmitted over 5G fosters ever more automated and customized products and services. Another will be greater intimacy and humanity in people's digital experiences, as AI augments human capabilities and creates closer alliances between humans and machines. Together, these impacts will drive another: big increases in productivity and work/leisure bandwidth, with people freed up to pursue activities they're really interested in.

AI also has a role to play in cybersecurity in a 5G world. This is because AI and ML offer organisations powerful new tools to protect their systems from those with malicious intent — enabling them to combat the increasing sophistication of tools used by the attackers. In PwC's view, the most effective defence will involve using AI to sort through data and flag it for human analysis, with the human analysis feeding back into AI to improve its future predictions. This virtuous circle will provide the best defence for critical systems — creating a robust, secure basis for innovation to deliver the full benefits of 5G across all use cases.

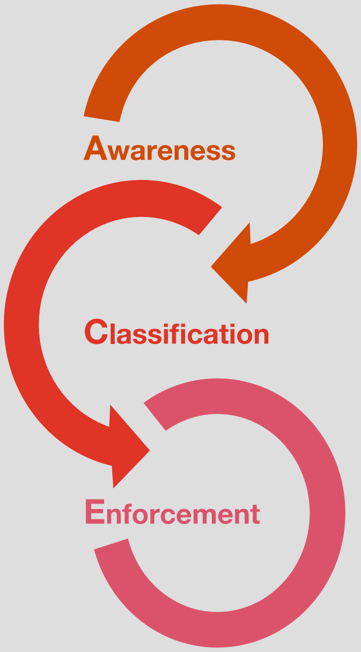
A vital first step towards protecting any network against cyber threats — 5G included — is to understand where vulnerabilities might arise.

Applied properly, the strategy will help organisations to work collectively to secure the 5G environment, while not overly impacting the ability of each business in the 5G ecosystem to serve its customers and interact with partners. A proven way of operationalising this strategy is to adopt an identity-driven model known as a zero-trust architecture (ZTA). This is a comprehensive information and infrastructure security model that addresses the 'who, what, where, why and how' when critical data and infrastructure assets are being accessed.

Under a ZTA, security capabilities are deployed to enforce policy and protect all users, devices, applications and data resources, and the communications traffic between them, regardless of location or connection method. The ACE model (awareness, classification, enforcement) depicted in Figure 1 can help companies to implement their ZTA.

Figure 1. Adopting a zero-trust philosophy for 5G

A comprehensive information and infrastructure security approach must address who, what, where, why and how critical data and infrastructure assets can be accessed. This identity-driven approach, commonly referred to as a zero-trust architecture (ZTA), deploys security capabilities to enforce policy and protect all users, devices, applications, data resources and the communications traffic between them regardless of location or connection method, using the ACE model.



Profile. Discover and profile every endpoint and application on your network.

Assess. Ascertain security posture of the devices.

Identify. Know which users and devices are connected and how.

Learn. Continuously assess behaviours of devices and users through monitoring and logging.

Weigh. Assess the value/importance of assets, data and applications to be protected.

Risk score. Assign a risk score based on the impact of a security exposure.

Assign to groups. Map data, users and endpoints to data classification buckets/groups.

Prioritise applications. Use business prerogatives, data classification buckets and associated risk score to generate security policies that align with the prioritisation.

Restrict. Determine access eligibility and enforcement boundaries based on security policy.

Isolate. Determine how compromises and violations will be detected, contained and isolated.

Notify. Provide mechanism for notification of breaches and security violations.

Segment. Define framework for identity-based segmentation of applications, endpoints and users.

Enforce. Implement identity-aware controls at enforcement boundaries based on defined security policies.

Source: PwC analysis

Resilience by design

Companies that are supported by a zero-trust approach and its related architecture are well placed to build and embed cyber resilience in the 5G era. Valuable guidance on how to achieve this is available in PwC's latest Digital Trust Insights report, which is based on survey data from more than 3,500 businesses worldwide.

The study finds firms that exhibit a high level of resiliency ranked in the top 25% in three areas related to developing resilience strategies. Fundamentally, their emphasis on 'resilience by design' puts this group far ahead of the rest. As a result, they are able to do the following:

- **Improve visibility of data assets.** Resilient companies consistently track how their data assets and existing processes are affecting the core of their business. The Digital Trust Insights report found that 91% of high-resilience companies maintain an accurate inventory of assets and refresh it on a rolling basis, compared with just 47% of the other respondents. It's critical that this inventory includes work with third parties, especially if the business works with a range of vendors — as it almost inevitably will in a 5G world.

  Companies on the wrong side of the resilience divide can take action to catch up. By automating a real-time asset inventory and mapping the process for ongoing and accurate visibility across the network, organisations with low resilience can begin to address their vulnerabilities.

- **Test their tolerance.** Resilient companies look at the big picture and recognise their tolerance level for handling risky situations. We discovered that, when facing disruption to their critical business operations during a cyberattack, less than one-third of the enterprises in our study were able to defend themselves using impact tolerance, or the maximum impact to business services that a firm is prepared to tolerate in the wake of operational disruption. The other firms participating in our study — notably including the largest organisation surveyed — put their critical business services in jeopardy when such a disruption occurred.

  By identifying critical business services, using metrics to define their impact tolerance, and then testing and mapping the impact tolerances to business services, companies can prepare to handle incoming threats.

- **Adapt and refine.** Resilient companies continuously evolve their business strategies. By improving the visibility of their data assets and testing their tolerance level, organisations put themselves in the high-resilience league. However, when facing the rapid development of technology, we found that only 34% of highly resilient companies adapt to the changes underway.

  To ensure all-around protection, one-third of all highly resilient organisations refine their resiliency as they adopt new technologies. These firms often rely on a dedicated team to monitor the performance of core assets and IT dependencies, and can quickly and consistently redesign business services based on lessons learned from disruptions caused by cyber issues. As part of this preparedness, companies should adopt advanced threat-hunting capabilities that leverage automation and orchestration.

Together, these three characteristics enable an organisation to shift from a traditional disaster recovery/business continuity model to resilience by design — which is something that many companies will need to do as they navigate the COVID-19 crisis recovery. Resilience by design is already proven to secure organisations, operations and systems against cyber threats — and is as relevant and effective in a 5G environment as in any other.

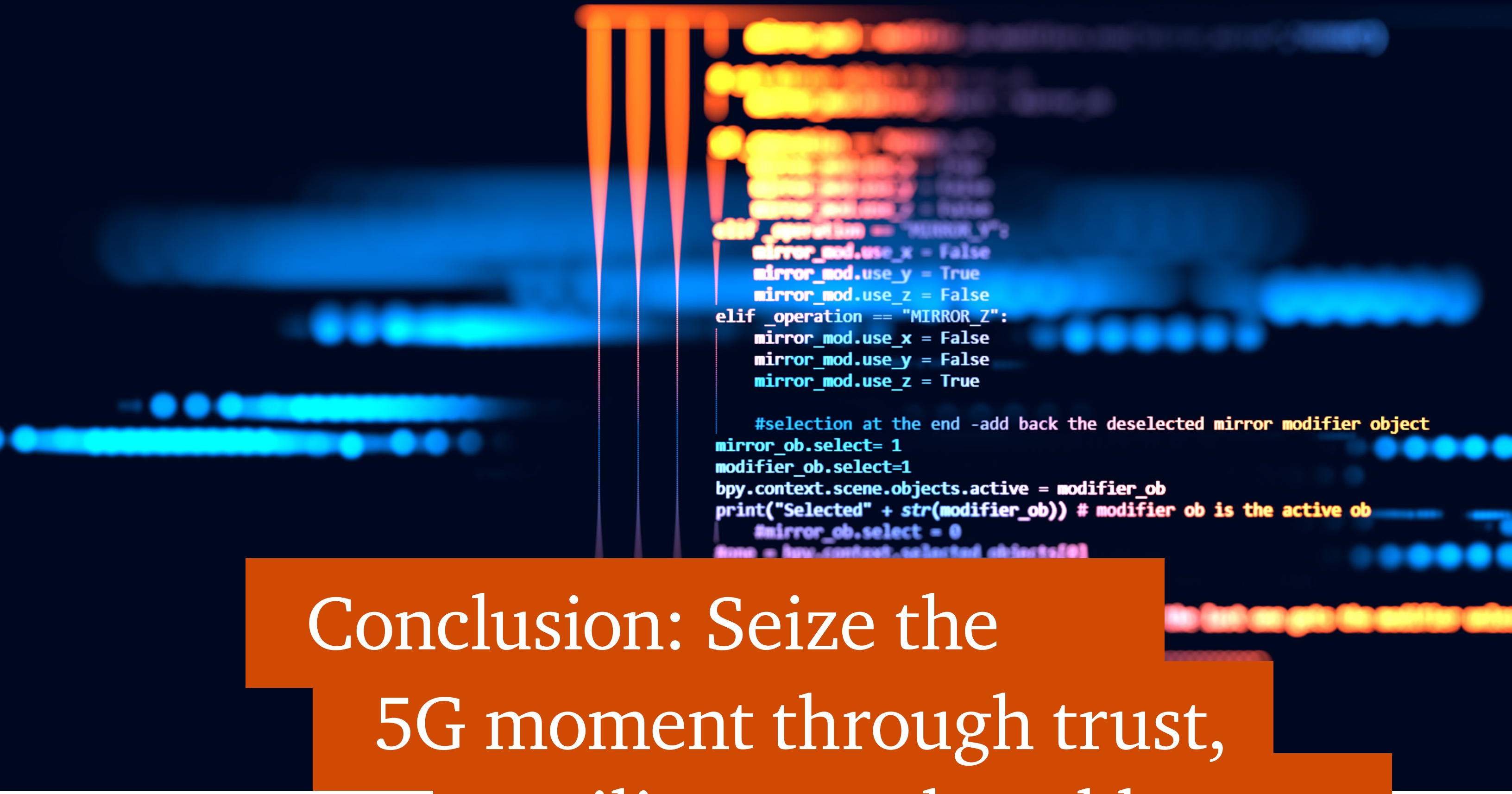
Companies on the wrong side of the resilience divide can take action to catch up. By automating a real-time asset inventory and mapping the process for ongoing and accurate visibility across the network, organisations with low resilience can begin to address their vulnerabilities.

Smart cities: Enabling the future of urban environments

With urban populations continuing to grow rapidly, putting increasing strains on traditional infrastructure, the race is on to transform existing cities around the world into smart cities. The British Standards Institute (BSI) defines a smart city as "the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens." This is a very apt definition, as it highlights how smart cities represent the marriage of physical and digital in the creation of cyber-physical systems (CPSs).

Digitisation can enhance a vast array of urban systems to meet citizens' needs more effectively — most obviously in areas like transport and facilities management in buildings, but also in systems such as energy, water, public safety, waste management and pollution control. There is also potential to help manage public health emergencies, such as the coronavirus pandemic, by enabling modelling, detection, and prediction, and providing governments with real-time data to inform their decision-making process. 5G will help to realise the full potential of the smart-city concept by delivering an ultra-high-speed, low-latency platform to underpin these services.

Keeping smart-city systems secure will clearly be vital, both in terms of operating infrastructure and citizens' personal data privacy. This can be achieved by ensuring all smart-city systems and connectivity are designed, assessed and conditioned from the ground up with security at their core, under a zero-trust approach.



```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Conclusion: Seize the 5G moment through trust, resilience and enablement

It is often claimed that 5G will transform the world, but it's important not to get swept away in the hype. Although the world is clearly changing, what's really driving that change is the near-universal availability of smart connected devices. The network through which those devices connect is just one part of this new environment, albeit an important one.

That said, there's no doubt that the advent of 5G represents a shift in the cybersecurity landscape. It will be the medium through which the workflow and decision chains of the automated interconnected components in tomorrow's critical industrial and societal networks will flow. And without 5G, the growing millions of connected devices — especially those involved in applications such as self-driving cars, where low latency and connectivity at high speeds are prerequisites — would be effectively useless. 5G is certainly not overhyped in terms of being the 'connected' component of many smart connected devices.

Against this background, nobody would question that effective cybersecurity across the 5G ecosystem is non-negotiable. However, it's important to note that many of the security vulnerabilities commonly laid at 5G's door are not actually specific to the 5G technology itself. If devices, encryption algorithms or AI engines connected to 5G networks are penetrated or compromised, it's a problem for 5G operators and users. But it's not specifically a 5G problem. Effective security in a 5G world requires every participant in the value chain to play their part. That's why we propose a zero-trust approach backed up by 'resilience by design' — putting cybersecurity at the centre of every 5G deployment.

To do this, company leaders will need to focus on three fundamental pillars of security: *trust*, to drive adoption of cybersecurity measures; *resilience*, to prevent, ride out and recover from disruptive attacks; and *enablement*, to move fast to overcome new and existing threats. These pillars are the foundation of a sound cyber strategy and will ensure that companies can roll out 5G quickly and safely, enabling individuals, business and society as a whole to enjoy the potential of this powerful new tool confidently and securely.

Contacts

To find out more about how PwC can support your journey to a 5G-enabled future, please contact us.

Technology, Media and Telecommunications

Wilson Chow
Global Technology, Media and Telecommunications Leader
Partner, PwC China
+86 755 8261 8886
wilson.wy.chow@cn.pwc.com

Kirolous Zikry
Senior Manager, PwC UK
+44 77 2563 3388
kirolous.s.zikry@pwc.com

Cybersecurity & Privacy

Richard Horne
Partner, PwC UK
+44 77 7555 3373
richard.horne@pwc.com

Marin Ivezic
Industrial and IoT Cybersecurity
Partner, PwC Canada
+1 416 687 8672
m.ivezic@pwc.com

Peter Durojaiye
EMEA Cyber Impact Center
Director, PwC Hungary
+36 70 685 0360
peter.a.durojaiye@pwc.com

Grant Waterfall
EMEA Cybersecurity and Privacy Leader
Partner, PwC UK
+44 77 1144 5396
grant.r.waterfall@pwc.com

www.pwc.com