Vanilla+

THE GLOBAL VOICE OF
TELECOMS IT

Issue 2 2024
ISSN 1745-1736

EXCLUSIVE NOKIA CYBERSECURITY REPORT

COVER INTERVIEW
iconectiv's Mike O'Brien explains how verified identity will slam the door on fraud

Amdocs on why modernisation projects go wrong

PLUS MWC BARCELONA 2024 event preview ■ MATRIXX Software asks if you're ready for the era of digital monetisation ■ Mobile industry warns fraudsters it's got their number ■ Dell and Nokia expand private wireless partnership ■ Amdocs unveils CPQ Pro ■ How will cellular operators use GenAI? ■ Kyivstar selects Comarch for field service maintenance ■ Why networks demand different security approaches to traditional cybersecurity for IT apps ■ GSMA and IBM collaborate on AI training ■ News, Features and Interviews at www.vanillaplus.com

THE GLOBAL VOICE OF TELECOMS IT

Kaleido Intelligence

Accurately Measure the Size of Your Market with the Latest CONNECTIVITY DATA HUB UPDATE

Based on primary research with **1000+** companies and covering **60+ markets,** this comprehensive historical & market forecast database includes 5G, Cellular IoT, eSIM, Mobile Security & Fraud, Cellular LPWAN, Private Networks, Direct-Satellite and Vertical Connectivity

NEW KEY REPORT INSIGHTS

OVER 500 MILLION LTE-M CONNECTIONS FORECAST IN 2028

1.4 BILLION eSIM/iSIM SHIPMENTS ANTICIPATED IN 2028

DIRECT-TO-SATELLITE CONNECTIONS TO REACH 160 MILLION IN 2028

GLOBAL CELLULAR IoT CONNECTIONS EXPECT TO REACH 6.2B IN 2028

To access the research or request a sample visit our Research Centre: www.kaleidointelligence.com

ANALYST REPORT

How will telco networks manage cybersecurity as the threat surface expands?

IN THIS ISSUE

Cover sponsor: Your business and your customers need to confidently access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services, digital identity and numbering intelligence helps you do just that. In fact, more than 5,000 customers rely on our data exchange platforms each day to keep their networks, devices and applications connected and two billion consumers and businesses protected. Our cloud-based information as a service network and operations management and numbering solutions span trusted communications, digital identity management and fraud prevention. For more information, visit **www.iconectiv.com**. Follow us on **X** and **LinkedIn**.

AI has lots to learn so enjoy the gestation period

Artificial intelligence has suddenly entered a new wave of prominence thanks for ChatGPT and Open AI. The potential to automate tasks such as writing school assignments, partially preparing legal positions and relying on large language models (LLMs) to get that next presentation roughed out is exciting. Such advances will free up time for other activities but there's a danger that we're expecting too much, too soon. AI still has a lot to learn before we trust it to run networks, initiate network functions and handle mission critical communications

George Malim
managing editor

Telecoms has always had to contend with what I think of as pregnant years. This describes the gap between a technology emerging and becoming widely understood and when it hits full commercialisation and delivers on its promise. This disconnect between pre-arrival hype and post-development maturity typically goes on for so long that I've become bored long before the first fruits of the concept become reality.

5G, for example, has taken so long to complete its gestation from exciting new high-speed ultra-low latency technology to an actually available service that supports hugely important applications, that I've not only started wearing reading glasses but had to buy stronger ones in the interim. It's important that we don't over-expect when it comes to early iterations of AI while also maintaining enthusiasm for how it will transform telecoms.

AI is a fantastic tool to power seamless automation of new networks which will rely on elastic scalability to spin capacity up or down according to demand. We'll see network slices being activated to support specific services at specific times and AI, allied to rich operational data, is the means by which billions of network iterations will be handled automatically. Importantly, there is no alternative to automation here – cost must be controlled and hyperscale volumes must be handled.

This is why AI is so significant and is attracting so much intelligence across the telecoms industry. The destination is clear but we must avoid the temptation to place too much reliance on a technology that currently can barely turn in a decent term paper. It's wrong of us to ask AI to enable automated operations of future networks today. It has much to learn and we must stretch out and wait for that learning to take place. The gestation period will be at least elephant-long.

Enjoy the magazine!

George Malim

MANAGING EDITOR
George Malim
Tel: **+44 (0) 7930 301 841**
george@vanillaplus.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: **+44 (0) 1732 808690**
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: **+44 (0) 1732 807410**
c.jameson@wkm-global.com

DESIGN
Jason Appleby
Ark Design
Tel: **+44 (0) 7801 817 139**

PUBLISHED BY
Prestige Media Ltd. Suite 138, 80
Churchill Square, Kings Hill, West
Malling, Kent ME19 4YU, UK
Tel: **+44 (0) 1732 807410**

PRESTIGE MEDIA LTD.

VanillaPlus magazine is published as a digital edition at least 4 times a year. It is available free of charge to all readers worldwide, at the publisher's discretion. To subscribe **free of charge** go to: **www.VanillaPlus.com**, click the "Subscribe" tab on the Home Page and answer the questions shown. The Publisher reserves the right to alter or end this free offer at any time without notice. No guarantee is stated or implied. You can unsubscribe at any time by emailing **subscribe@vanillaplus.com** with UNSUBSCRIBE in the Subject line.

Dell and Nokia extend partnership for telecom and 5G innovations

Dell Technologies and **Nokia** have announced the extension of a partnership to use each company's expertise and offerings, including infrastructure from Dell and private wireless connectivity from Nokia, to advance open network architectures in the telecoms ecosystem and private 5G use cases among businesses.

As part of the agreement, Nokia will adopt Dell as its preferred infrastructure partner for existing Nokia AirFrame customers, offering Dell's technology as the infrastructure of choice for telecoms cloud deployments. Nokia and Dell will help transition existing AirFrame customers over time to Dell's infrastructure portfolio, including Dell PowerEdge servers, purpose built for modern telecoms network workloads from core to edge to RAN. The Nokia Digital Automation Cloud (NDAC) private wireless solution will become Dell's preferred private wireless platform for enterprise customers' edge use cases. The companies will work together to integrate Nokia's NDAC solution with Dell NativeEdge, the edge operations software platform, to provide a comprehensive, scalable solution for enterprises.

"Through our collaboration, Nokia and Dell Technologies will harness each company's expertise and expanded distribution to simply and quickly scale modern telecoms networks and private 5G use cases," said Dennis Hoffman, a senior vice president and general manager of the Telecom Systems Business at Dell Technologies. "With our decades of digital transformation experience, we're ready to work together with Nokia's customers to continue their network cloud transformation journey on the industry's top selling compute platform."

Dennis Hoffman, Dell Technologies

Nishant Batra, the chief strategy and technology officer at Nokia, added: "This strategic partnership will make both companies more flexible and able to better address future customer needs. Dell's digital transformation expertise and global scale, services and support will provide a seamless transition option for Nokia AirFrame customers, and Nokia's vast experience in the design, deployment and operation of high-performance public and private mobile networks will provide Dell's customers with a comprehensive, scalable private wireless solution."

Amdocs unveils CPQ Pro for CSPs

Amdocs has announced Amdocs CPQ Pro, its next-generation configure-price-quote software that empowers communications service providers (CSPs) to deliver advanced enterprise services to businesses of all types. This solution harnesses the power of generative AI capabilities, enabling CSPs to offer highly tailored and efficient services.

Underpinned by Amdocs' generative AI platform, amAIz, CPQ Pro aligns with Amdocs' strategy of advancing generative AI co-pilot use cases across the communications industry, bringing reduced time to market, enhanced efficiency and next-level customer experience through service differentiation across its products and services portfolio. In addition, this launch strengthens Amdocs' CES portfolio by using its existing partnerships with **Microsoft** and **NVIDIA**, expanding the integration of generative AI capabilities.

"We believe in generative AI's ability to transform the telecoms industry and enhance experiences for enterprises and consumers alike," said Anthony Goonetilleke, the group president of technology and head of strategy at Amdocs. "CPQ Pro is one of the industry's first generative AI-infused CPQ applications meticulously crafted for CSPs. It empowers our customers to capture and accelerate enterprise revenue opportunities, extending beyond just connectivity to encompass new digital and e-commerce services and network-based value-added services."

NEWS IN BRIEF

Vodafone Romania partners with Ericsson for 5G RAN

Vodafone Romania has selected **Ericsson** as a 5G radio access network (RAN) partner for upgrading its current infrastructure and for 5G deployments. As part of the six-year agreement, Vodafone Romania will also use Ericsson's RAN technology to enhance its existing mobile network which means that Vodafone Romania customers will benefit from faster connectivity speeds, low latency and more reliable and secure network performance.

The partnership is part of Vodafone Romania's multi-year investment plan for infrastructure upgrade and development, in line with the company's mission to help enable the digital society.

"In support of a digital society, building a future-ready, secure, energy-efficient network is crucial," said Nicolae Vîlceanu, the chief network officer at Vodafone Romania. "The partnership with Ericsson gives us the technological fundamentals in our endeavour to roll-out 5G standalone (SA) networks with tremendous impact for our customers: residential users, companies and authorities, in terms of speed, low latency and diversity of use cases. It is also helping us upgrade existing RAN infrastructure in order to provide fast, reliable services in the transition to 5G Standalon and harness our potential as a services innovator for the digital, green society we envision."

Comarch partners with Kyivstar to enhance field service maintenance in Ukraine

Comarch has signed a deal with **Kyivstar**, to help the Ukranian CSP improve field service maintenance activities. With 24.3 million mobile network subscribers and a further 1.1 million internet customers, Kyivstar faced the task of modernising and updating field service processes. The company is responsible for ensuring the smooth running, maintenance and preventive upkeep of equipment serving 1.1 million apartments and more than 32,000 objects in the radio access network (RAN) network in Ukraine.

The scale of the project meant that it was no longer feasible to rely on existing field service maintenance procedures to effectively achieve the set goals. By implementing the Comarch Field Service Management product, Kyivstar will be able to streamline and automate processes, optimising maintenance and route planning for technicians while tracking tasks in real-time and gaining the data necessary for the timely and accurate analysis of tasks in hand.

Tymoteusz Wrona, the head of telco business unit consulting at Comarch, said it had taken two years of discussions before the contract was signed earlier this year. "We listened carefully and actively to Kyivstar, ensuring that we understood their requirements before tailoring a field service management offer using Comarch FSM," he said. "In this way, we were able to best address our Ukrainian neighbour's business needs and help them meet their goals."

Tymoteusz Wrona, Comarch

Vitaliy Gubenko, the head of the operational support department at Kyivstar, said: "With more than 24 million subscribers, we have responsibility for a huge portfolio of telecommunications and IT services. For 25 years, this has been our priority – but as a socially responsible company, it is even more important during wartime. Comarch will lead us through the process of streamlining and automating the processes behind our expansive and geographically wide-ranging field service management activities while providing a product that was designed specifically to meet the challenges faced by Kyivstar in this area." ■

Telstra expands partnership with MATRIXX for enhanced charging and 5G support

MATRIXX Software has announced that **Telstra** has completed a multi-year expansion with the company. Telstra initially deployed MATRIXX in 2014, and this latest agreement expands MATRIXX's role to include operations support previously managed by other vendors. The expansion also provides additional charging capabilities for a wide range of consumer and enterprise services, including key features such as dynamic slice monetisation, to comprehensively support 5G standalone (SA).

"The success of our T25 vision is dependent upon the partners who make it possible," said Shailin Sehgal, a Telstra product enablement technology executive. "MATRIXX has been a valued partner of Telstra since the very beginning of our digital transformation journey. This latest agreement is a testament to the strength of the relationship we have built over those years and shows how close collaboration and trusted partnerships can deliver benefits to every part of the business."

The MATRIXX platform has continuously scaled in response to Telstra's digital journey, with MATRIXX providing converged monetisation for Telstra's post-paid services on both 4G/LTE and 5G networks across consumer, SMB, IoT and enterprise services.

Glo Gordon, MATRIXX Sotware

"As one of our earliest customers and investors, Telstra has played a pivotal role in making us the company we are today," said Glo Gordon, the chief execvutive of MATRIXX Software. "At every part of our business, we have been laser-focused on, and relentlessly committed to, the success of our customers around the globe. This latest expansion is not only a reflection on that commitment to Telstra but a validation of our belief that our customers' success is our success." ■

NEWS IN BRIEF

SmarTone boosts network performance with Infovista's Ativa solution

SmarTone has transformed its customer experience and network performance by implementing Ativa, **Infovista**'s automated assurance solution, across its 3G, 4G, 5G and IMS network. SmarTone, committed to delivering consistent and exceptional experiences to its customers, sought an innovative assurance solution to optimise service and customer monitoring, enhance troubleshooting capabilities and elevate overall customer satisfaction.

Ativa has equipped SmarTone with enhanced monitoring and troubleshooting capabilities, offering valuable insights into voice and data, including intelligence on over-the-top (OTT) applications delivered over mobile and 5G fixed wireless access (FWA) broadband. Its flexibility has facilitated the delivery of customised solutions aligned with SmarTone's specific requirements, while its support for Open APIs has enabled integrations with third-party systems, ensuring a smooth export of data and analytics. ■

GSMA and IBM collaborate on AI Training and Foundry Generative AI programmes

The **GSMA** and **IBM** have announced a new collaboration to support the adoption and skills of generative artificial intelligence (AI) in the telecoms industry through the launch of GSMA Advance's AI Training programme and the GSMA Foundry Generative AI programme.

The AI training programme, the first in a new series of courses by GSMA Advance, seeks to prepare telco leaders for the AI-era and bridge skills gaps in the telecoms industry, by equipping members with skills and knowledge to help effectively use Gen AI technologies utilising watsonx, IBM's AI and data platform with AI assistants.

"Artificial intelligence provides the telecoms industry, and the societies it serves, with huge opportunities to launch new services, improve connectivity and customer experience," said Alex Sinclair, the chief technology officer at the GSMA. "Overall, it's estimated that AI could contribute US$15.7 trillion to the global economy by 2030. However, it's critical that AI is democratised to ensure that all parts of the connectivity industry and their customers, wherever they are in the world, benefit. Bringing operators access to AI tools and knowledge, alongside the necessary skills, access and training, is key to achieving this."

Alex Sinclair, GSMA

Stephen Rose, the general manager of global industries at IBM, added: "IBM will provide critical support to this training for the telecoms industry through this collaboration with the GSMA. Generative AI can create opportunities for communication service providers as they look to optimise current processes, and like the GSMA, our goal is to offer this technology within the industry." ■

American Tower to sell ATC India operations in US$2.5 billion deal

American Tower has entered into a definitive agreement with **Data Infrastructure Trust** (DIT), an Indian infrastructure investment trust sponsored by an affiliate of Brookfield Asset Management. As per the agreement, DIT will acquire 100% of the equity interests in American Tower's operations in India, known as **ATC India**.

DIT currently houses Brookfield's telecoms tower businesses in India through Summit Digitel and Crest Digitel. Total cash proceeds to American Tower at closing, subject to certain pre-closing terms, would potentially represent up to approximately INR 210 billion, or US$2.5 billion at current exchange rates. The transaction, which reflects the completion of the previously announced review of American Tower's operations in India, is subject to customary closing conditions, including government and regulatory approvals, and is expected to close in the second half of 2024.

Total cash proceeds include an enterprise value on the ATC India operations of approximately $2.0 billion, plus a ticking fee that accrues from 1 October 2023, to the date of closing. Proceeds associated with the enterprise value assume the repayment of existing intercompany debt and the repayment, or assumption, of the existing India term loan, by DIT.

In addition to the total potential cash proceeds, American Tower will also retain the complete economic benefit linked to the optionally converted debentures (OCDs) issued by **Vodafone Idea**. Furthermore, American Tower will be eligible to receive future payments associated. ■

NEWS IN BRIEF

Actis-Led consortium acquires Telekom Srbija's macro tower portfolio

An **Actis**-led consortium has acquired the macro tower portfolio of **Telekom Srbija**. The carved-out portfolio is comprised of approximately 1,800 macro towers and is well placed for further commercialisation and expansion. As part of the transaction, an independent tower company has been established, fully controlled by Actis, which has entered into a long-term master services agreement (MSA) with Telekom Srbija as the tower company's anchor tenant and important partner for future growth. The MSA contemplates build-to-suit (BTS) commitments to further expand the platform's reach and to accommodate new telecommunications technologies that will be rolled out in the region.

Jaroslava Korpanec, a partner and head of Central and Eastern Europe at Actis, commented, "We are very proud to lead this groundbreaking investment, marking the first transaction of its type in the Balkans. This investment strengthens Actis' strategic decision to expand its strategy into the CEE region following on investments made in 2022 in the energy sector in Romania and Bulgaria. We look forward to a long-term relationship with Telekom Srbija in developing a first-class tower portfolio in the region." ■

Whether it’s spam or scam, verified identity will slam the door on fraud says iconectiv

Consumers and businesses are under constant attack from fraudsters who are targeting mobile devices to breach the security of bank accounts, harvest sensitive personal information and misuse and abuse the global communications network. When the high-capacity, globally ubiquitous network that connects everything and everyone is under relentless assault, businesses and the telecoms industry as a whole are under pressure to protect the digital identity of themselves and their customers.

At the epicentre of trusted digital identity lies the phone number. Serving as today’s de facto personal identifier, the phone number keeps commerce flowing, businesses running and consumers engaged. Mike O’Brien, the executive vice president of business development at iconectiv, explores the role of the phone number for verifying identity, how the industry is protecting it and what’s needed next ►

SPONSORED INTERVIEW

We now live in a world where so much of what we do – from making purchases to financial transactions, data sharing and more – relies on global communications networks

George Malim: With the uptick in digitalisation, all eyes seem to be on digital identity. What are some of the biggest challenges companies face regarding verifying identity and navigating fraud?

Mike O'Brien: We now live in a world where so much of what we do – from making purchases to financial transactions, data sharing and more – relies on global communications networks. No matter the flavour of information exchange, we appreciate the sheer convenience that our mobile devices provide us. But when there is so much at stake, think personal details, financial information and more, this convenience also brings tremendous risk and responsibility. Because of this, one of the biggest challenges with digital identity is truly knowing the 'who'.

It is a challenge for companies and consumers alike. For companies, the challenge lies in verifying the identity of consumers they're trying to do business with. For example, does the company really know who is making a transaction? For consumers, the challenge is to ensure that they're interacting with a brand they know and trust. Who really sent the text message they received about their bank account?

Interestingly, while most people are careful in sharing certain personal information, the phone number is handed out readily – often as a matter of ease or necessity. That is because most companies rely on phone numbers to deliver critical information, sell and support products and services, and facilitate a myriad of consumer engagement and conversational commerce transactions. To further complicate things, by their very nature, mobility and cloud communications make digital identity verification and validation more complex as the virtual aspect requires different ways of determining whether a person or a business is who they say they are. This is due to several factors, such as the volume of data, the frequency of changes, unreliable or aged data and the numerous inaccuracies in non-phone number data. As a result, it is not surprising that the phone number is one – if not the most – important signal in the complex identity verification process.

GM: Talk more about the different factors of digital identity verification. Why is the phone number so critical?

MO: A digital identity is comprised of several data points or signals, such as name, physical address, email address, IP address, biometrics and phone number. Unlike the phone number, though, there are a lot of inconsistencies with these other data points. Take one's name for example. It's not always in a Latin character set or may contain other special characters like an apostrophe, which makes it harder to consume and requires more resources and manual intervention to verify. The same thing goes for physical addresses, where there is no standard format from town to town, city to city, county to county, or even country to country. When it comes to reliance on newer technologies like biometrics, there are varying rules and inconsistencies across the globe with regard to practices, legalities and authorised uses.

The phone number, however, is easier to manage and understand. For instance, the syntax is consistent and well-documented. Phone numbers can reference intrinsic information, such as the carrier of record, which service provider currently owns it and whether it is fixed, wireless or ▶

Because mobile devices are now the gateway to financial services and ecommerce, mobile devices and numbers are now one of the key targets for fraudsters

VoIP. Phone numbers are absorbed into existing systems easily and consistently. Not to mention that, given number portability, an individual can essentially keep their phone number for life.

We, as an industry, are in a great position: We oversee one of the most critical components of the digital identity mix. But this position comes with great responsibility. Since connectivity is at the core of the main commerce and communication vehicles that everyone knows, loves and uses, the integrity of the phone number must continue to be protected.

GM: Can you talk a little more about what businesses and consumers are dealing with on the fraud front, and how the phone number is being used to combat it?

MO: If history has shown us anything, it's that fraudsters will exploit any channel for financial gain. They've gone from stagecoach robberies in the wild west, to piracy on the open seas, to forgery and impersonation. The common thread with all these tactics is that when there's money to be made, bad actors will always find ways to manipulate and take.

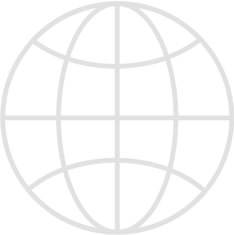
Because mobile devices are now the gateway to financial services and ecommerce, mobile devices and numbers are now one of the key targets for fraudsters. Fraudsters know that the phone provides the convenience and simplicity that consumers demand, which is the reason why spoofing and illegal robocalling have become some of their weapons of choice, and the reason why research shows that more than a third of reported fraud to the US Federal Trade Commission, for example, starts with texts (22%) or phone calls (20%).

Not only are fraudsters fast, flexible and far-reaching, but the phone number is tied to every part of the digital identity lifecycle from authentication to account creation, to engagement, to transaction and event monitoring.

As I previously mentioned, the ability to determine and verify the who is incredibly important. Knowing the who is at the root of why Know Your Business (KYB) and Know Your Customer (KYC) processes – which were once critical regulatory requirements confined to the financial sector – are now essential across most industries for verifying identities and effectively managing risk.

While the KYB verification procedure is used when businesses want to authenticate their outbound communications; KYC is a system focused on verifying an individual consumer's identity and ensuring that the customer is who they say they are. Fortunately, for both KYB and KYC, this can be accomplished via the concept of verifiable digital identity, which involves an understanding of the data associated with phone number and correlated business or individual information.

Here's an example. One of our customers, a major global corporation in the financial services sector, is utilising phone number porting data to combat account takeover fraud. This critical data enables the company to flag if phone numbers have been recently ported from one communication service provider (CSP) to another. If the phone number has recently been ported, in combination with other data, this could be a signal of risk. The ▶



financial services company can then do a deeper dive into determining whether the phone number information provided by the customer is accurate, that it's a legitimate customer transaction or that there may be a risk that that the number has been taken over by a fraudster. By having access to this critical porting data, the business can make sure they have the right info to make the right decisions in the moments that matter.

GM: Shifting gears a bit, can you talk a little about illegal robocalling and what's being done to combat that?

MO: With robocalling, the main concern isn't so much about receiving spam calls as it is about receiving scam calls. Spam is irritating while scams are malicious, executed by fraudsters always willing to exploit any channel they can to deceive people. Regardless of whether it's a spam or scam call, many people are reluctant to answer the phone, creating frustration between brands and their end consumers.

One of the issues is that when traffic comes through it may look local, but it's not. In the UK, for example, you could get a phone call from a UK number that has actually originated from a call centre in another country. It may be presented as valid, but it could be a scam or spam. The same holds true for conference calls that terminate or originate between countries – the conference bridge could call from a UK number even though the call originated on a conference platform in the US.

Fortunately, the telecoms industry is uniquely positioned to help mitigate this issue, protecting digital identity and mitigating fraud. For instance, the ability to brand or verify a business caller ID could be useful in combatting this issue. As could the continuation of frameworks like STIR/SHAKEN – which, is a suite of protocols and procedures designed to authenticate the originator of phone calls in order to combat illegal robocalls. This means the originating and terminating networks know where the call is coming from and where it is going, which can be useful for identifying fraudsters.

Some of these types of measures are bearing fruit. In December 2023, the US saw the lowest level of robocalls since early 2022, which stands at a noteworthy 20% below the monthly average for 2023. Many view this as a viable blueprint for what can be done in other countries across the globe.

But beyond cutting down on illegal robocalls and the obvious benefits to the telecom industry, standards like STIR/SHAKEN can also lead to marketable services and new revenue streams. While STIR/SHAKEN was initially widely viewed as a regulation that CSPs needed to comply with, the communications market has evolved their thinking to focus on how to apply similar call authentication protocols globally. There are also discussions to provide business call authentication and verification, so consumers have more confidence that a business caller is who they say they are — ultimately helping consumers make an informed decision when deciding to answer the call or respond to a text.

We believe verifying identification through phone numbers presents a significant opportunity for CSPs, especially if there can be global collaboration. We are seeing the beginning of this movement within specific countries or by individual CSPs that are offering premium services related to enhanced call security, personalised authentication and advanced communication features. Eventually that verification must be cross carrier, cross country and across the globe.

We believe verifying identification through phone numbers presents a significant opportunity for CSPs, especially if there can be global collaboration

GM: How is iconectiv poised to support these – and other needs – in the identity verification battle?

MO: We have several different roles as a provider of trusted, neutral, third-party data exchange platforms within the communications ecosystem. In the case of robocalling, iconectiv has the tools to address verification challenges; and we're a provider of data to digital identification companies. Likewise, digital identity providers are also customers of ours. A key goal for us is to help expand and emphasise the opportunity for the communications market because it has a huge opportunity to monitor and protect the trust inherent in its own market as well as others.

We are also trusted to run number portability platforms and are the policy administrator for STIR/SHAKEN in the US, where we support the cryptographic encryption of digital handshakes that validate digital identities.

In general, our focus is on global collaboration and sharing trusted, authoritative information between networks. While everyone has their own authentication platforms, we need to think bigger. For iconectiv, this means continuing to forge relationships across the entire ecosystem – CSPs, regulators, enterprises and others – for the good of the whole. We are continuing to focus on developing platforms to combat scams, spam and fraud, and remaining vigilant in our efforts to foster a trusted global communications ecosystem that can continue to rely on the phone number as the most trusted and reliable signal to verify digital identities globally. This success in the communications market can be extended to establish a reusable digital identity framework across other industries. ■

www.iconectiv.com

How to enhance global security by utilising phone number data to counteract fraud

iconectiv has developed its Digital Identity Solution for the financial services industry to help combat the risk of fraud. The solution relies on porting data for identity verification, fraud prevention and risk management

Challenges:

- Businesses – and financial services companies in particular – are challenged to manage numerous, complex and often inconsistent data sources, files and formats to verify the identity of customers in an effort to manage risk and prevent fraud. This extensive constellation of data is exponentially more complicated for companies operating on a global scale.
- While an individual's digital identity is comprised of several data points or signals, their phone number has quickly emerged as the key personal identifier globally.
- At the same time, sophisticated fraudsters and hackers have targeted phone numbers as an entry point to commit fraud, often leading to fake accounts and purchases, negatively impacting consumers and businesses' bottom lines.

> **"The one constant across the entire globe is the phone number."**
> **– financial services customer**

Solution:

- iconectiv's Digital Identity Solution flags recently ported phone numbers, offering a reliable method to verify the accuracy of a phone number for identification purposes.
- iconectiv data is presented in a canonical format, covering numbering and country codes for countries and territories worldwide.
- Numbering data set contains valuable metadata such as the carrier of record, and line type (mobile, fixed or VoIP).

> **"The phone number is crucial, the phone number is the future; the phone number is a meaningful asset across every single type of identification verification."**
> **– financial services customer**

Results:

- Reliable, real-time data to verify the attributes about the phone number ownership is an important identification signal for the financial services industry.
- Simplified delivery of critical data that requires less computing power to analyse.
- Increased fraud prevention and risk management, including minimised errors and instances of false verification or fraud.

SPONSORED CASE STUDY

Financial service companies are faced with an evolving cartel of fraudsters and hackers looking to exploit their business through any channel possible. Research from **Statista** shows nearly half of all fraud reported to the US **Federal Trade Commission** starts with texts (22%) or a phone call (20%). For financial services companies, when that happens, revenue dips, brand reputation diminishes, customer satisfaction wanes and regulatory intervention soars.

At the same time, **Juniper Research** has reported that mobile phones will become the primary source of identity for over three billion people globally by 2024, further cementing the phone number as the de facto personal identifier to defend and protect commerce, privacy, data and reputation.

Several signals make up one's digital identity, with the most common attributes including name, email, physical address, IP address and the phone number. The phone number, however, is widely viewed as the single most important piece of data in the complex and layered process used to verify identity. Not only are phone numbers harder to generate as compared to a signal like an email address, but they are location-oriented, and come with a history of which phone company was assigned the number, which one currently services it and line type.

In addition, the dataset for phone numbers is easier to manage and analyse at a global scale. Phone numbers follow a consistent format as opposed to names and addresses, which can vary drastically from country to country, requiring more engineering and computing power to normalise the datasets.

Identity verification for fraud prevention and risk management

Every day, businesses and consumers count on phone numbers to facilitate billions of transactions that are predicated on knowing who is on the other side of the line. Furthermore, most multi-factor authentication efforts, including those delivered by text message, are linked to the phone number so protecting this critical digital identity signal is of utmost importance.

Financial services companies rely on iconectiv – a neutral, trusted guardian of critical mobile number data globally – to help mitigate fraud by using the phone number as a key digital identity signal. The iconectiv digital identity portfolio eliminates uncertainty by providing extensive, authoritative and accessible dynamic phone number intelligence, data sets and other identification signals.

iconectiv's comprehensive digital identity solution facilitates porting and enables number management by using iconectiv's industry-standard data. In addition to helping with fraud mitigation and risk assessment by delivering authoritative, port-corrected data from 100+ nations spanning six continents, the TruNumber platform provides a comprehensive global database of all assigned phone number ranges with the specific, approved number format by country, and covers 245 ISO Country Codes for countries and territories worldwide. As a result, global companies are armed with the critical data insights needed to protect themselves and their customers every step of the way – from registration to login to transaction and event monitoring to ongoing engagement. Shareable across internal teams and departments, this important data is easily ingestible into existing systems, processes and workflows. As a result, financial services companies can quickly categorise customers into the correct risk ratings, save valuable resources, reduce customer friction and make more informed assessments to protect their business and their bottom line.

To learn more about iconectiv's digital identity solution,
visit **www.iconectiv.com/digital-identity**

"When we're talking to our customers, they have operations on every continent. They're doing something everywhere and they want to make sure that the product that they're receiving works equally well in the United States, as it does in the UK, as it does in UAE. That's something that iconectiv provides that is of high value."

– financial services customer

Fraudster warning: The mobile industry has got your number

With fraud continuing to impact telecoms operators, financial services institutions, many other businesses and huge numbers of consumers, digital identity verification is becoming a routine part of commerce and our lives. The phone number is becoming an increasingly robust means by which digital identity can be verified

The scale of the fraud problem is amply demonstrated by the scope of the efforts being made to prevent fraud. **Juniper Research** predicts that the number of digital identity verification checks will surpass 70 billion in 2024; growing 16% on the previous year's number of 61 billion. This figure is only set to grow further by 2028 with digital identity check volumes being dominated by the Far East and China which will account for 25% of checks, western Europe, which will account for 24% of checks, and North America, which will account for 17% of checks.

Of course, as the landscape tightens against fraudsters in one region they will shift to a less-protected territory to continue their activity before taking a new approach and starting the vicious cycle all over again. Fraud is nothing new and is a routine part of modern life. **Experian** in its latest UK Identity and Fraud report has uncovered that 69% of organisations experienced 'significantly' or 'somewhat' higher losses from fraud in 2023 compared to 2022. This demonstrates continued momentum is with the fraudsters as highly-organised, professionally operated crime groups target customers.

That's becoming an even greater concern for organisations such as financial services providers which suffer reputational as well as business losses when fraud occurs. Certainly, Experian's research revealed that UK consumers feel under attack. 35% of consumer respondents cited in its report feel that they are now more of a target for fraud than they were a year ago. Identity theft is perceived to be the greatest threat.

Organisations, however, are far from unarmed when it comes to fighting back against fraud. Identity verification – which incorporates multiple techniques and technologies – works by analysing data from numerous sources, such as from online identities and cross referencing it with trusted data sources, such as the credit bureau, to gauge the likelihood that customers are who they say they are.

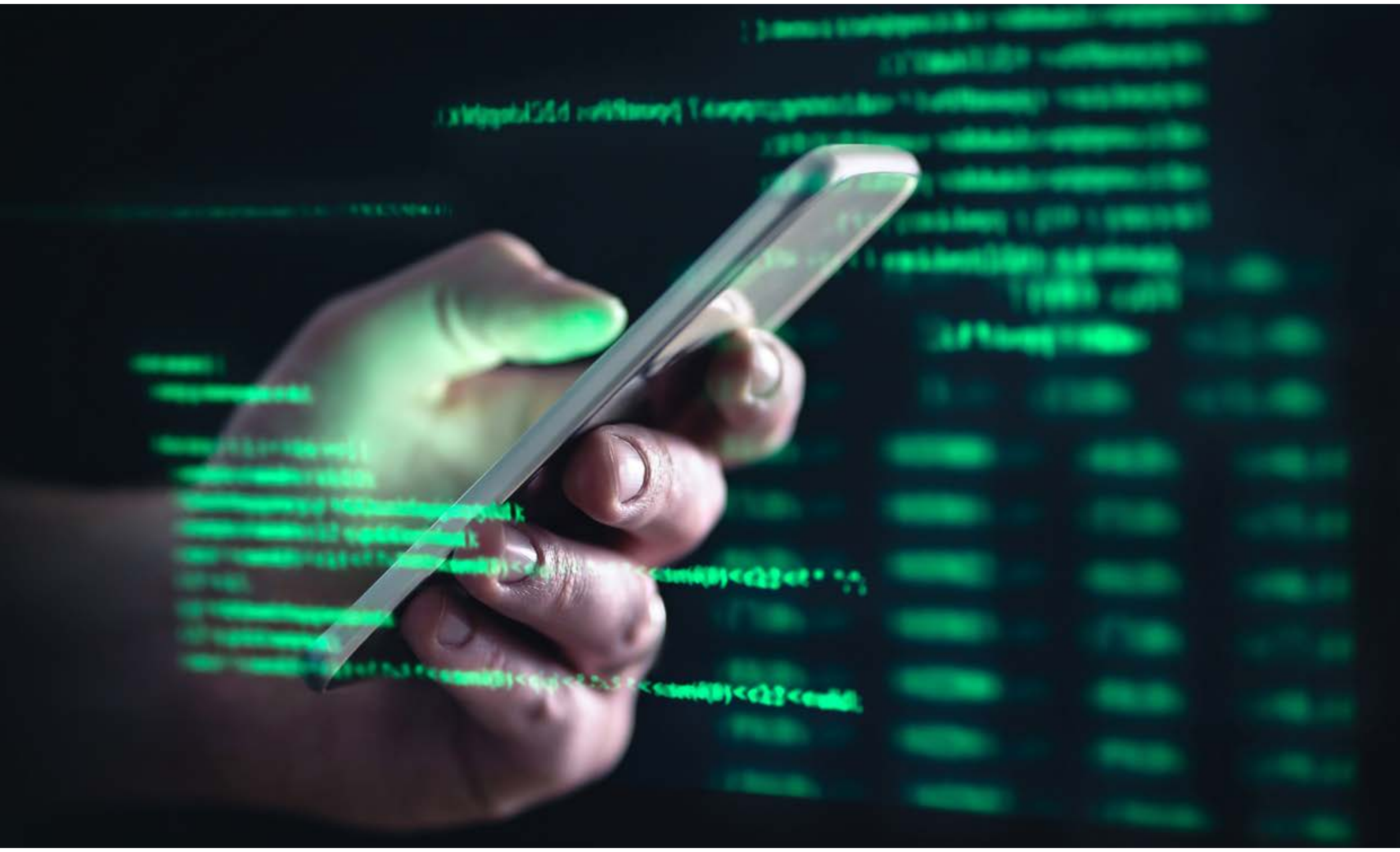
The technologies and processes that enable effective, remote digital identity verification are many and varied, but fall into two key categories.

1.Online variants of traditional identity verification approaches
This includes the ability to check customer details, such as name, address and date of birth, against trusted data sources, for example banking records – or to verify their identity documents remotely using technologies such as artificial intelligence and machine learning.

2.Analysis of data relating to customer behaviour, devices or online footprints
The use of data analytics to understand more about the device a customer is using is becoming a popular tool for combatting fraud. The location and the IP address of the device can also be used to ensure data points are consistent with behavioural biometrics. On one level, something as basic as knowing whether a phone is present at the same location that a credit card is being billed can highlight a potential fraud but greater intelligence can be applied to know, for example, that a middle-aged man is unlikely to be purchasing a teen beauty product. Other behavioural routines can also be analysed and enable an organisation to analyse how customers initiate sessions online, how they hold and use their mobile devices, or whether they have other online accounts that match their online identity information. Combining incremental inputs such as these helps build up a picture of whether an online identity is genuine or fake.

Mobile network data

An extremely valuable source of information is consumers' mobile phone identities, which include their name, address, device details and other information that is typically associated with a phone number or contract. The global mobile identification ▶



market is expected to register a CAGR of 8.9% during the forecast period (2022-2027), reports **Mordor Intelligence**. During the pandemic, there was a sudden push towards digital transformation, with online marketplaces adopting digital transformation programmes to serve customers and maintain operations. The transition towards digital has led to the significant need for mobile identification.

Mobile ID largely relies on biometric technology to function. Any smartphone or tablet can be used as a multi-factor authentication device with the help of biometric software that converts cameras and microphones into biometric sensors. Mobile identity is increasingly supported by strong authentication factors, with fingerprint sensors and facial recognition becoming almost common components of modern smartphones.

The on-demand economy companies are shifting towards mobile ID scanning and verification to solve problems related to financing, licensing, compliance and the personal safety security of both employees and customers. This instant identity verification has triggered the market vendors to offer a mobile, fast and easy-to-use platform. They also feature smart/connected databases for quicker identity verification results.

Mobile identity

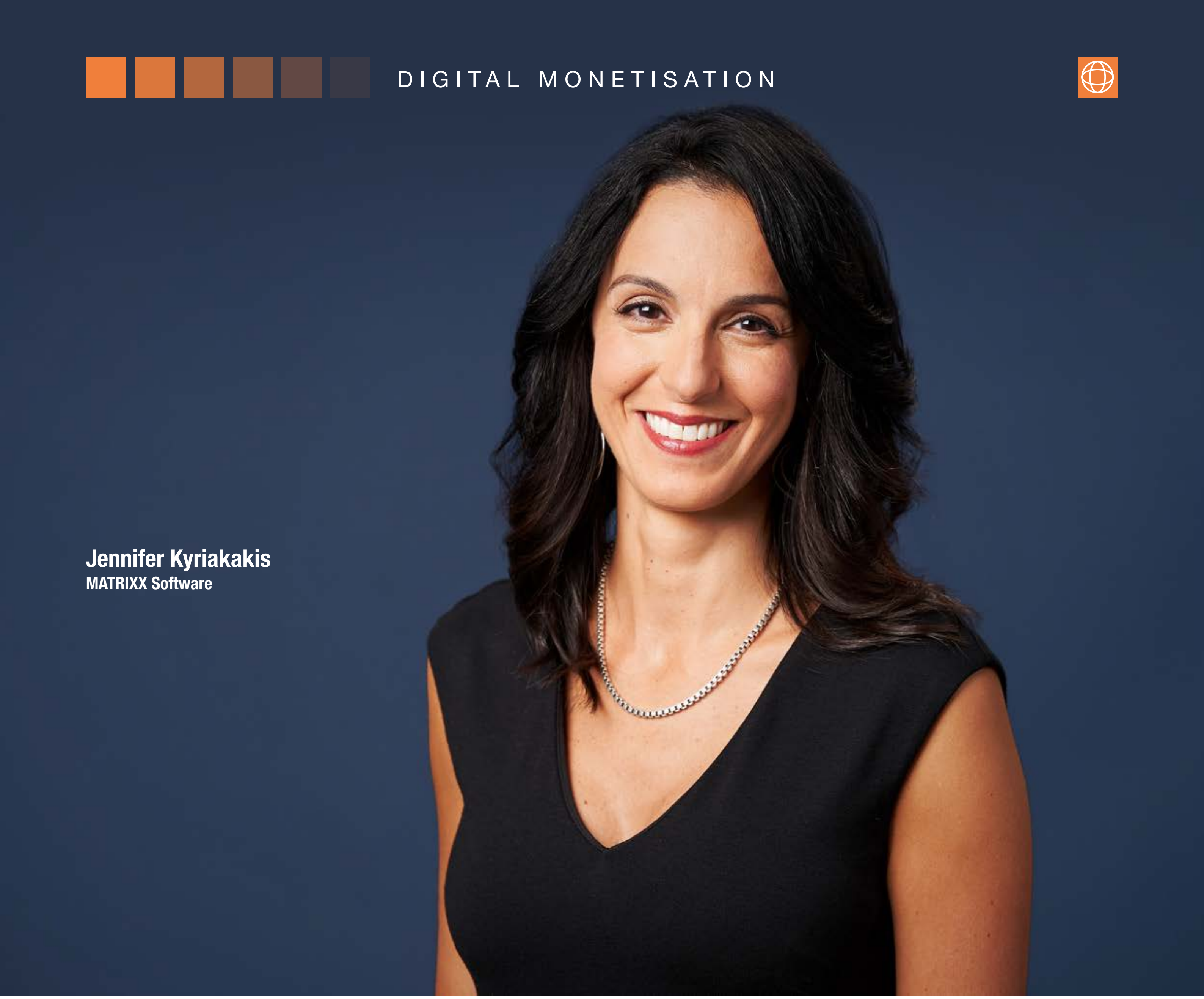
The ubiquity of the mobile phone makes it an ideal tool for verifying identity and Juniper Research has projected that mobile phones will become the primary source of identity for more than three billion people by 2024. Number portability now enables users to retain the same number for life and that means it is recognised as a globally cemented personal identifier.

“When it comes to verifying a digital identity, the phone number is the single most important piece of data that businesses use to verify a person or company,” says Peter Ford, the executive vice president of Information Services at **iconectiv**. “Phone numbers are easier to manage because the syntax of the number is consistent on a global scale. In addition, how they are managed, distributed and created is unique and comes with history and metadata that makes it a meaningful asset across every type of identity verification.”

In addition to delivering the convenience and simplicity that consumers demand, mobile phone numbers provide the reliable, verifiable data that businesses need and the global ubiquity that other identity signals cannot replicate. As such, ensuring the integrity of the phone number remains intact is of paramount importance.

“While phones were initially established to be a more efficient and accessible way to communicate, they have organically evolved as a consistent indicator used to defend and protect commerce, privacy, data and reputation globally,” adds Ford. “That is why it is of the utmost importance that the communications ecosystem bands together to create an impenetrable force to keep out bad actors, who use the reach and anonymity of hiding in a digitally connected society for their personal gain.” ■

The on-demand economy companies are shifting towards mobile ID scanning and verification to solve problems related to financing



Jennifer Kyriakakis
MATRIXX Software

The era of digital monetisation is here - are you ready?

As communication service providers (CSPs) search for ways to differentiate themselves, delivering digital-first customer experiences continues to be a top priority. For the last decade, transformation has focused mostly on customer engagement layers and supporting omnichannel experiences such as discovery and purchasing.

Increasingly, however, CSPs are focusing on transforming systems and processes across the complete end-to-end customer lifecycle, particularly when it comes to billing and payments. The industry is evolving past connectivity and to digital services; in the same vein, customer relationship management has evolved to become digital engagement. The third wave of transformation is coming, and it's from billing and revenue management to digital monetisation, writes Jennifer Kyriakakis, the founder and chief marketing officer of MATRIXX Software ▸

The drivers behind that third wave are painfully clear. Every unexpected charge, every billing error, every confusing invoice erodes customer trust and increases the risk of churn. For too long, legacy billing processes have acted as a drag on CSPs' financial performance, limiting agility, driving up the cost of revenue management and becoming a major contributor to customer dissatisfaction. Billing consolidation projects, while giving the impression of positive change, simply address the symptoms, not the underlying causes of fundamentally broken billing processes.

The impact of those broken processes on customer satisfaction and the operational costs to CSPs cannot be underestimated. A recent report from **STL Partners** highlighted that close to 50% of calls to CSP call centres are billing-related, costing a typical telco approximately US$60m per annum.

> **For a typical telco, at least 40% of customer calls are billing related - most of the time it's the number one issue they complain about**
>
> Principal Transformation Office, Tier-1 operator, EMEA

It also highlighted how some 60% of new go-to-market offers are delayed by billing efficiencies, resulting in a 33% drop in profits for projects that are delayed by six months. Even worse, in a number of cases, excessive delays result in projects being cancelled before launch.

> **It's the complexity of doing operations from the whole number of systems we have - billing and rating platforms - that make it highly inefficient in how we operate**
>
> Technology and Innovation Manager, Tier-1 operator, EMEA

Overall, the report highlighted some US$168m of annual savings, equivalent to a near 2% uplift in EBITDA for a typical CSP, from the implementation of a modern, streamlined monetisation approach.

> **Before I wouldn't be surprised if 50-60% of calls were billing related, but now everything is transparent, so we never have compaints about this. It's a gamechanger**
>
> Principal Transformation Office, Tier-1 operator, EMEA

A different operating model

Older, established industries, such as CSPs, are (in)famous for lagging behind in modernising both internal operations and customer-facing processes. Some have even met their potential demise (think taxis). There is no easy way to transform a business when confronted with decades of IT buildouts that have resulted in layers of complexity and Chinese walls around organisations and their associated data and processes.

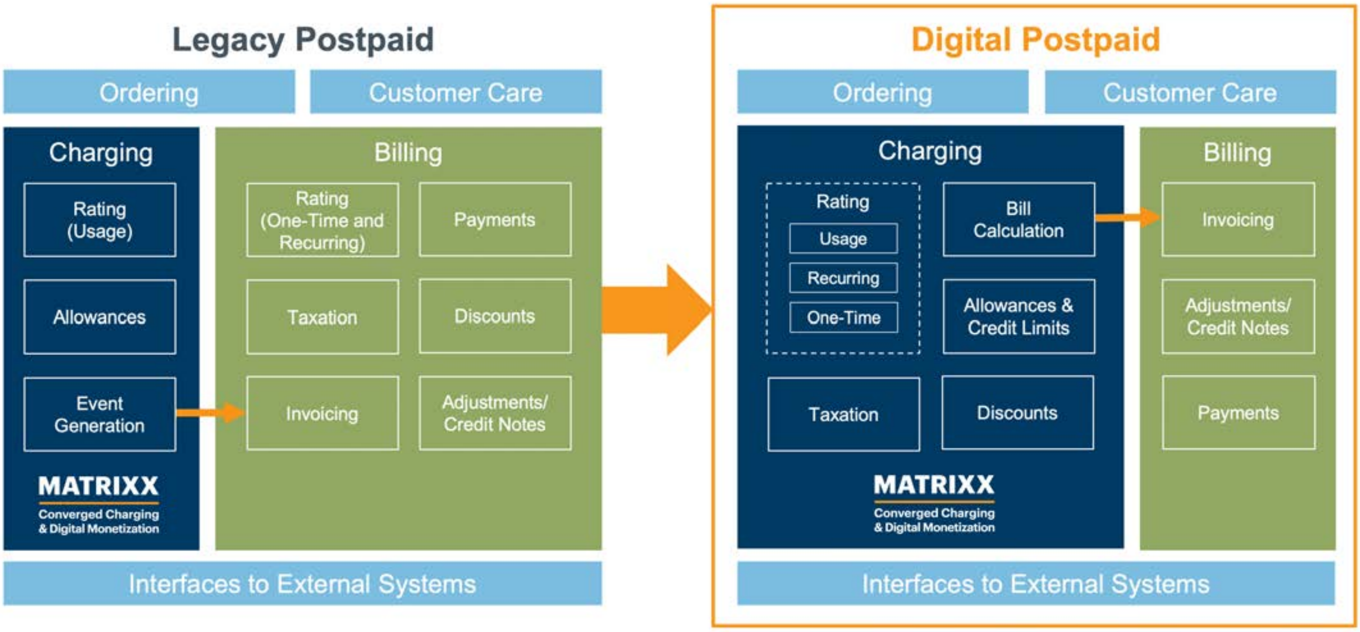
The reality is, if a telco could design customer and business operations today, it would look very different than it did ten or 20 years ago. And with 5G, cloud and AI technologies, some greenfield players are getting to do just that. Whether they are serving mass market consumers, like **Verizon Visible** or **AWS**, offering private 5G as a service to businesses, newer entities are embracing a simpler, leaner approach to billing operations that will give them a competitive advantage. So how can the established service provider possibly compete?

Adopting a digital monetisation approach accelerates a CSP's evolution to a modern digital business architecture, helping solve key challenges currently impacting both existing margins and new services/revenue. As CSPs evolve their go-to-market around cloud, data and 5G service offerings, this becomes the time to redesign the processes that directly impact how revenue will be generated from new services.

Digital monetisation 101

Digital monetisation provides real-time processing and visibility of all customer charges. Customers have full transparency into accounts, balances, services and usage, creating a more optimal customer experience. This is achieved through a unified set of monetisation services that are used ▶

Every unexpected charge, every billing error, every confusing invoice erodes customer trust and increases the risk of churn



By calculating all charges in real-time, service providers are improving how fast the bill is generated

across customer types, networks, payment methods and lines of business. For CSPs, the benefits are enormous, from the shedding of extraneous systems and processes to the ability to gain customer insights that are actionable in real-time. This evolution requires a rethink of how to transform passive utility-style billing and collections processes into active engagement that will drive more revenue while simplifying and improving how customers buy, use and pay for products and services.

How does digital monetisation work?

The traditional functional demarcation between billing, charging, ordering and care is changing. Charging is assuming more charge calculation functions, while billing (and invoicing specifically) provides bill-cycle-run functions, like billing quality assurance (QA), invoice generation and integration with other systems, including bill formatting and financial reporting.

The diagram above shows the shift of functions from the legacy, bill-cycle-driven billing system to the real-time charging system. There is a centralisation of all rating — usage, one-time and recurring. Taxes and discounts are now calculated in real-time, adding significant value to the information presented to customers during the billing cycle.

A key part of digital monetisation is real-time charge calculation, including taxes and discounts. Charges are calculated when incurred. For an existing plan, the monthly charge is calculated at the start of the bill cycle rather than the end, and this could be any charge, including for subscriptions, contracts or devices.

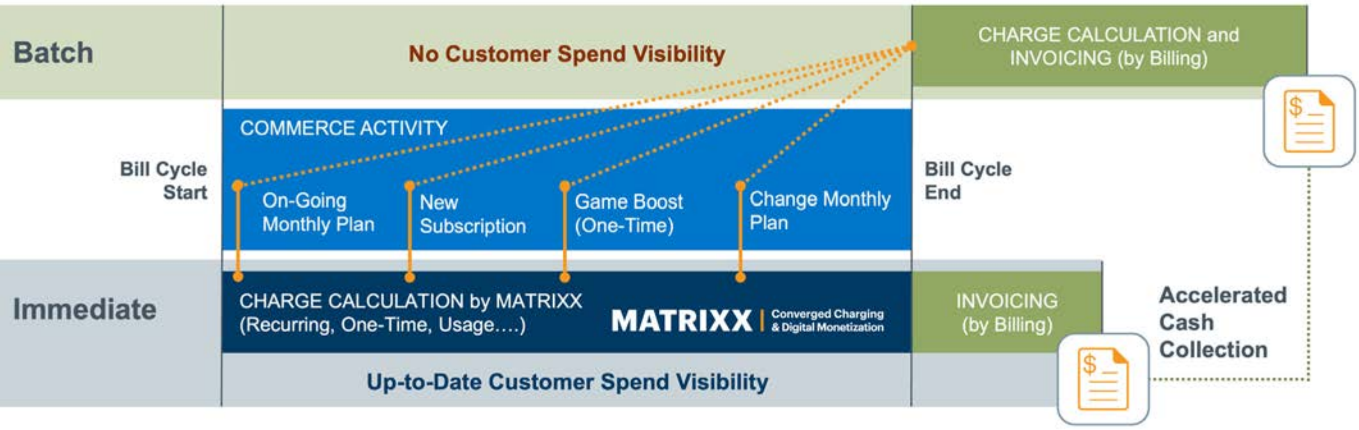
For one-time activities like a game boost or a new or changed plan, the charges are calculated when ordered. This is how service providers can achieve transparency and immediacy, giving the customer their up-to-date spend visibility at all times, and giving care staff the same visibility.

By calculating all charges in real-time, service providers are improving how fast the bill is generated and, therefore, cash is collected, with some validation and QA activities undertaken throughout the period, reducing the end-of-cycle load. Overall, the bill cycle process is simpler as it just needs to process charges already created and passed to it. The principle of immediate charge calculation versus the traditional, typically end-of-month, bill-cycle batch calculation is illustrated below:

How do we get there from here?

Change is uncomfortable, even sometimes painful. Do you remember going to the bank every time you had to deposit a cheque? Now, you take a picture of it through an app. Banks in North America spend upwards of US$80bn a year on technology upgrades, a staggering number. But would you use a bank that still forced you into a branch or to an ATM to make a deposit?

As CSPs continue to invest billions in 5G, edge, cloud and AI, breaking down the barriers that ▶


Batch
No Customer Spend Visibility
CHARGE CALCULATION and INVOICING (by Billing)
COMMERCE ACTIVITY
Bill Cycle Start
On-Going Monthly Plan
New Subscription
Game Boost (One-Time)
Change Monthly Plan
Bill Cycle End
Immediate
CHARGE CALCULATION by MATRIXX (Recurring, One-Time, Usage….)
MATRIXX | Converged Charging & Digital Monetization
INVOICING (by Billing)
Accelerated Cash Collection
Up-to-Date Customer Spend Visibility

make it difficult and costly for consumers and businesses to sample, buy, change and pay for new services will be key to adoption and eventual return on investment. Existing billing processes and application architectures must change to enable simpler, more dynamic revenue generation processes.

Reusable processes that aren't hard-wired for a specific type of customer or service, and instead can be easily adapted and scaled, are necessary to monetise evolving product and customer portfolios.

Now is the time to rethink revenue management. Ditch the silos. Lose the complexity. Innovate beyond the limits of traditional billing by actively driving monetisation processes that engage the customer. Existing billing systems remain rooted in the past and obstruct telco operations. Digital monetisation delivers a deeper level of customer engagement with real-time insights paired with a simplified operating model, streamlining costs, accelerating go-to-market agility and cash collection and, crucially, putting the customer at the centre of the relationship. In doing so, this lays the foundation for the services that will define CSPs' futures.

MATRIXX Software is already undertaking this digital monetisation transformation journey with some of our customers around the world. If you'd like to explore more, visit: **http://www.matrixx.com/customers/**. ■

Now is the time to rethink revenue management. Ditch the silos. Lose the complexity

How cellular operators can use generative AI

Generative artificial intelligence (GenAI) is the use of machine learning models to produce various types of content including text, images, programming code, audio, video or other forms of media in response to prompts and by applying rules based on the data that models have been trained on. It is a broad term to describe an AI system whose primary function is to generate content and similar outputs. This is different from other types of AI, like discriminative AI which focuses on tasks such as classifying or identifying content, writes Jim Morrish, the founding partner, and Suruchi Dhingra, the research director, of Transforma Insights

This isn't a new concept, but it has garnered a lot of attention in the last year or so because of the mass adoption of models like ChatGPT, DALL-E and others. The training data sets, and the number of parameters used in the training of such models, has also increased enormously in the last couple of years. Moreover, until now companies have used AI to predict or identify patterns, but generative AI takes this concept a step further by generating outputs in formats that are easier for users to interact with, including text, video and images.

Emerging use cases are diverse

Generative AI can be deployed to support several enterprise functions, with the most prominent being marketing and sales, customer service operations, IT processes (such as application development), and product R&D. Generative AI also has potential in the context of HR, legal, supply chain, risk and compliance areas and together these contexts are next tier of priority use cases for early adopters. **Figure 1**, below, includes a summary of early-adopting functional areas and the use cases that **Transforma Insights** has identified as typically being utilised in those functional areas. ▶

Figure 1: Early adopting functional areas and associated generative AI use cases

[Source: Transforma Insights, 2024]

Functional Area	Use Case
Marketing	Offering personalised recommendations Creating advertising material content (including text and images)
Sales	Synthesising purchase orders and generating quotes Drafting personalised emails for sales leads
Customer Service	Summarising or transcribing customer interactions Supporting product search and shopping assistance on e-commerce platforms Personalising recommendations such as financial advice, health plans, product offers and more
IT Processes	Assisting with code development and testing
Finance	Generating financial insights and risk assessments for trading strategies Streamlining trade processing
Research and Development	Drug discovery Application discovery Chip design
Business Administration	Enterprise search and knowledge management

> **The first and most obvious way in which cellular operators can utilise generative AI is for supporting customer service, either using online or voice-based chatbots**

Jim Morrish
Transforma Insights

The use cases listed in **Figure 1** are currently being explored by companies across various industries at different rates. In pharmaceuticals, for example, generative AI has a strong potential to transform drug discovery processes by accelerating the development of novel molecules, disease target identification, and prediction of clinical trial outcomes. An initial focus in the IT sector has been to use generative AI to support the migration of programming code from legacy languages and environments to more modern implementations. Also in the IT sector, generative AI can be potentially used to support the semiconductor chip design process. Consumer packaged goods companies, meanwhile, have typically focused on deploying generative AI to enhance marketing, and multiple industries have experimented with generative AI to support customer service.

Use of generative AI in the telecoms sector

The mobile telecoms sector can benefit significantly from generative AI, and in many contexts. Those that have been explored so far include multiple use cases in customer service contexts, and also in sales and marketing, IT systems administration and knowledge management. Some of the leading use cases are discussed in more detail below.

The first and most obvious way in which cellular operators can utilise generative AI is for supporting customer service, either using online or voice-based chatbots. For many years, cellular operators have sought ways to automate customer service and so reduce costs and the advent of generative AI will allow for significantly more sophisticated solutions.

Generative AI can also play a role in customer service centres, supporting customer service agents. There are two main ways in which such support can be provided. It can take the form of prompted responses either to real-time customer enquiries or to written correspondence, which customer service agents can review and tailor before responding to a customer enquiry. Alternatively, generative AI can support the navigation of in-house knowledge to help customer service agents to respond to more unusual situations quickly and efficiently.

Still within the domain of customer service, generative AI can be used to help monitor customer service performance. Today customer service agents and customers both are often asked to review engagements after completion, providing ratings according to whether the issue motivating the customer enquiry was resolved efficiently or not. Generative AI techniques can be used to automate this process, providing unbiased and consistent results across all enquiries received (compared to the typically biased, inconsistent and partial feedback provided by human participants).

There is significant potential to use generative AI to support general sales and marketing of telecommunications services, including the generation of new messages targeted at specific segments and also identification of new segments.

Some leading cellular operators have used generative AI to help develop initial responses to requests for proposals (RFPs) received from enterprise clients. In this context, generative AI would typically be used to create an initial draft response, which bid managers or sales personnel can further refine before sending to a potential customer. This approach can save significant human resource by helping to automate many of the more basic and mundane aspects of responding to an RFP.

In technical support contexts, generative AI can be used to help migrate legacy software applications to new environments and also to test new software applications and support data translation between environments.

In a wider business administration context, generative AI can be used to support human resources and recruitment processes and even to help analyse legal documents and contracts. In the widest sense, generative AI can be used to support enhanced knowledge management and training within a cellular operator. Typically, generative AI techniques can help newly hired staff relatively quickly to reach levels of efficiency more usually associated with knowledgeable staff members who have been in place for years.

These are still early days

It's only a little over a year since generative AI hit the headlines with the release of ChatGPT based on the GPT-3 large language model and a rumoured US$10 billion investment from **Microsoft**. Since then, the technology has grabbed management attention and diffused across industries and functions at breakneck speed. We're still very much at an early stage of adoption though and it's clear that in future the technology will be used far more widely than it is already today.

Clearly, generative AI as a technology has huge potential to reduce costs and make key processes within adopting companies more efficient. But, for now, generative AI deployments typically focus on significantly increasing the efficiency of things that could already be done, rather than introducing new and truly transformative propositions. ■

www.transformainsights.com

Why modernisation projects go wrong

While large enterprises like banks and telcos often manage large legacy IT estates with thousands of applications, a common challenge emerges: many apps are outdated, no longer fit for purpose, and urgently require modernisation, writes Stephen Ellis, the division president and general manager of Amdocs Cloud

Modernisation can reduce tech debt, cut IT costs, improve the digital experience and enable innovation. Without modernisation legacy apps can place your organisation at a competitive disadvantage and constitute a security risk. Yet, due to limited budgets and the preference to take a manual approach, modernisation teams can touch only a fraction of these apps each year.

Indeed, research shows that 79% of modernisation projects fail to deliver the expected results. This is attributed to cost, complexity, scoping, skill gaps and project fatigue, amongst other reasons[1]. In contrast, based on our years of experience in modernisation projects, **Amdocs** contends that such failures are often due to a lack of focus on business value.

We hold that putting business value front and centre, and identifying the right areas to improve, is the essential first step towards a successful modernisation project.

The ‘wrong’ areas for modernisation

Choosing the correct focus for modernisation typically hinges on your modernisation team’s approach:

- **Comfort zone modernisation:** Focuses on areas where the modernisation team is skilled. Typically, this means no one sees the whole picture: database experts identify database problems; cloud experts diagnose cloud problems and so on. In addition, where teams possess specialised tools or processes, they’ll choose to target projects where those tools can be best utilised.
- **Technology-led modernisation:** This is where IT teams choose to deploy new and advanced technologies which will undoubtedly upgrade the tech. However, by not first identifying the organisation’s most urgent needs, there is no guarantee if the investment will positively impact the business.
- **If it’s broke, fix it modernisation:** When modernising an ageing system, it’s tempting to fix not just the core problem you had identified, but every problem that comes along the way. With this approach, teams simply move through the application making improvements and consuming budget. But this means any benefits are diluted by investment in less critical fixes, and crucially, the budget could be used up before the programme has achieved its goals.
- **Follow the money modernisation:** Some systems are better budgeted than others, resulting in preferential treatment from the modernisation team, even if their issues are less severe. Unfortunately, this is the reality in many organisations.

While teams may occasionally stumble upon the perfect solution, it’s more common for improvements to be isolated, where one application component is enhanced, but yields minimal overall business benefit. And often, this simply shifts the bottleneck to another area. ▶

Identify projects that address business needs

Amdocs has been helping customers with modernisation initiatives for over two decades. From our extensive experience, we've found that the key to modernisation success lies in aligning modernisation initiatives with significant, yet unmet business needs.

Selecting the right areas for modernisation begins with focusing on the business value, and then working to identify how to maximise the benefits that modernisation can bring. We call this approach **Value-Led Modernisation at Scale**.

> **The goal of modernisation must be to deliver maximum business value**

Value-Led Modernisation at Scale

Value-led modernisation prioritises business objectives, utilising AI and automation to achieve impactful outcomes.

At Amdocs, we evaluate all modernisation projects using these four fundamental principles:

Business-driven

Focused

Intentional

Continuous

- **Business-driven:** The purpose is to undertake projects that address specific business needs. The analysis and search for the right project begins with talking to the business.
- **Focused:** Analysis must be accurate and practical. The focus should go beyond app modernisation without overextending into a full IT stack review. The scope should remain within the four pillars of modernisation (see over), allowing for a broad, yet controlled assessment.
- **Intentional:** After identifying the right modernisation project, it's crucial to guard against modernisation drift. This means modernising strictly along the critical path, discerning which improvements to make, their sequence, and their budgetary implications.
- **Continuous:** Modernisation is not a one-time task but an ongoing process. It's essential to continuously re-evaluate and realign the modernisation roadmap with changing business needs. ▶

Modernisation at scale

For enterprises with thousands of legacy apps, manual analysis is clearly not a practical solution. This is where automation, machine learning and advanced AI tools come into play.

At Amdocs, we utilise automation to rapidly identify the quickest path to cost optimisation. This may include reallocating development resources, improving team skills and reducing turnover across application portfolios. As an example, our tooling can help assess and prioritise the disposition of applications for migration to cloud, evaluate technical debt and assess risk and business value. With effective use of these tools today, even small teams can rapidly perform tasks that would previously have taken armies of expert consultants. Amdocs' tooling is what makes modernisation at scale possible.

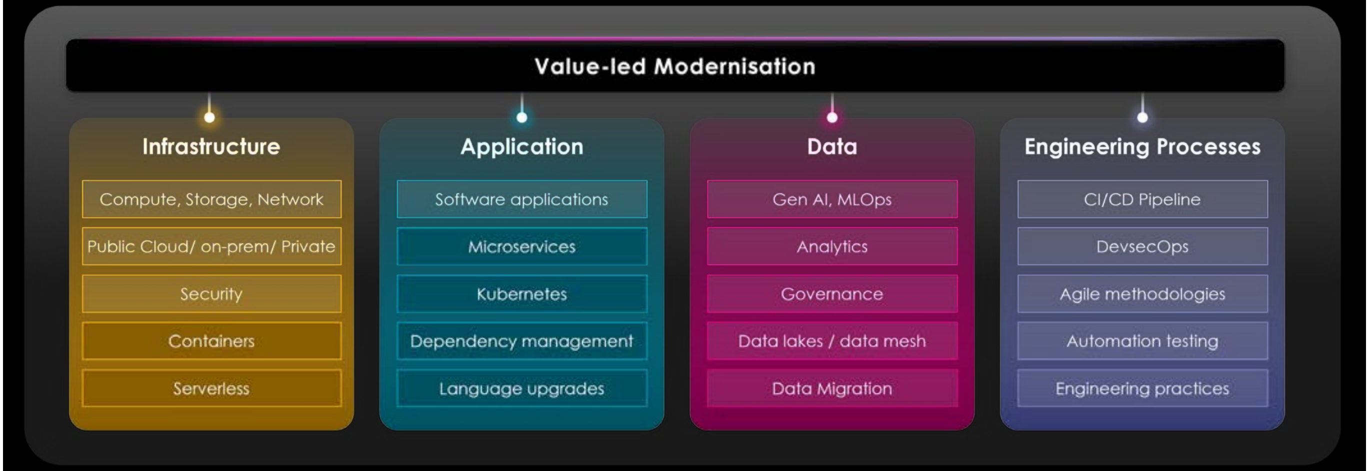
Still, tooling is only 80-90% of the solution. For example, it can identify deficiencies, but it doesn't tie those deficiencies to a specific business value. This is where consultants provide essential added value, combining automated code-level analysis with technical and business expertise. We analyse the information received and craft it into the optimal modernisation plan. We begin by conducting a brief evaluation, promptly followed by creating a modernisation roadmap that's designed to address specific business needs efficiently and cost-effectively. Then, we move rapidly to the operational phase, aiming to secure quick wins.

Tips for successful modernisation

- **Employ the right technology:** For example, in application migration to the cloud, Amdocs uses automation to create a roadmap and portfolio governance across hundreds of applications, sorting each into Rehost, Refactor, Rearchitect, Rebuild, or Retire buckets. We also navigate inside deeply complex applications to analyse internal structures, dependencies and communication patterns.
- **Touch only what needs to be touched:** With an identified business need in mind, employ automation to quickly identify the most efficient path to optimising costs, reallocating development resources, improving team skills and reducing turnover across application portfolios. Don't touch anything else unless it will help resolve an unmet business need.
- **Measure outcomes and know when to stop:** Metrics are crucial to determine when you've met the business need. But once target metrics have been met, stop modernising to avoid wasting resources.
- **Maintain a modernisation roadmap:** Value-led modernisation is an ongoing process that runs in parallel with the assessment of evolving business needs. Both business needs and technology are constantly changing. Have a prioritised roadmap of jobs to be done, and update it regularly.

Accurate scoping with the four cornerstones of modernisation

While modernisation programmes are often referred to as app modernisation, be careful this term does not restrict your view of what is required. Aligning tech capabilities with business needs extends well beyond simply refactoring applications or turning monoliths into microservices. Amdocs has identified four pillars of modernisation, where each pillar addresses a critical component of modern IT systems and business operations: ▶



Value-led Modernisation

Infrastructure	Application	Data	Engineering Processes
Compute, Storage, Network	Software applications	Gen AI, MLOps	CI/CD Pipeline
Public Cloud/ on-prem/ Private	Microservices	Analytics	DevsecOps
Security	Kubernetes	Governance	Agile methodologies
Containers	Dependency management	Data lakes / data mesh	Automation testing
Serverless	Language upgrades	Data Migration	Engineering practices

- **Infrastructure:** Refers to the foundational technology platforms on which applications and data reside. Modernising infrastructure improves performance, scalability and reliability. The ideal infrastructure for most companies is public cloud and includes compute, storage, networking and security. In some cases, it makes more sense to leave certain workloads in an on-prem environment.

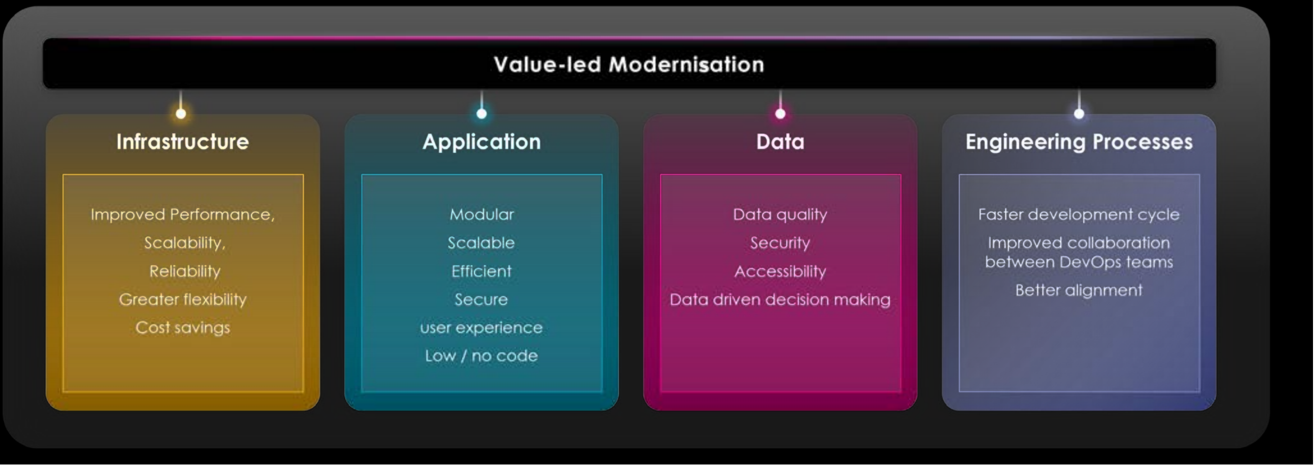
- **Applications:** Focuses on the software applications themselves – how they are designed, built and maintained. App modernisation can involve refactoring or rebuilding legacy applications to be more modular, scalable, efficient and secure. This is essential for integrating new functionalities, improving user experience and ensuring that applications can access the benefits of modern infrastructure, like cloud computing, as they work to deliver compelling business value.

- **Data:** Covers the way data is stored, processed, utilised and kept secure. Modernising data management and governance involves ensuring data quality, security and accessibility, enabling advanced analytics and data-driven decision-making. Businesses need to ensure that their data architecture supports big data technologies, real-time analytics, and is compliant with data protection regulations.

- **Engineering processes:** Refers to the methodologies and practices used in developing and maintaining software. Modernising engineering processes means adopting agile methodologies, DevOps practices and continuous integration/continuous deployment (CI/CD) pipelines, leading to more efficient and faster development cycles, improved collaboration between development and operations teams and better alignment with business objectives. Yet, this first requires getting developers to adopt these methodologies, which can be challenging.

Together, these four pillars move forward iteratively and cohesively. This means that investment that significantly advances one pillar while leaving others behind will often result in inefficiency, as the full benefits are only realised once all pillars are aligned.

The figure below lists the benefits from modernisation efforts invested in each pillar.


Value-led Modernisation

Infrastructure: Improved Performance, Scalability, Reliability, Greater flexibility, Cost savings

Application: Modular, Scalable, Efficient, Secure, user experience, Low / no code

Data: Data quality, Security, Accessibility, Data driven decision making

Engineering Processes: Faster development cycle, Improved collaboration between DevOps teams, Better alignment

Bringing it together

> **“ Assessing the four pillars above through a prism of delivering business value, will enable you to identify the right areas for modernisation.**

To achieve modernisation success, it’s essential to utilise advanced tooling, and assess and build coordinated modernisation programmes that reference all four pillars. With this approach you can fully realise the business benefits you are targeting.

Amdocs’ added value

After several decades of large-scale application and infrastructure development the need for modernisation has never been more pressing.

Done the wrong way, modernisation is a haphazard endeavor characterised by repeated failures and a few stellar successes. Done correctly, focusing on the business priorities, modernisation is a programme of steady improvement and wise investment that consistently aligns a company’s tech with its.

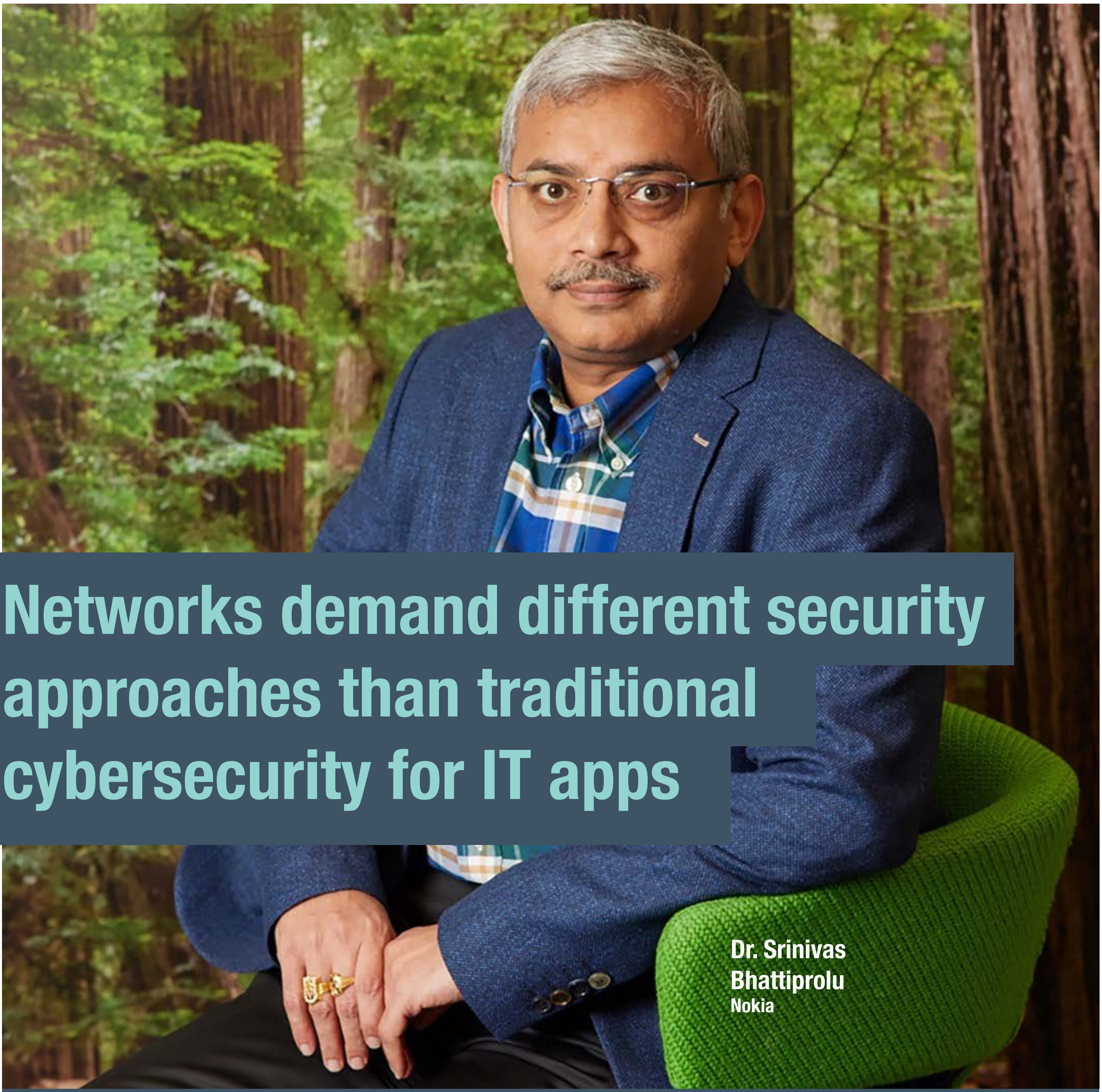
With approximately 30,000 employees across 90 countries, Amdocs offers deep technical knowledge and expertise in each of the four pillars of modernisation. These credentials are accompanied by an unmatched delivery record and a practical, business orientation.

Our Value-led Modernisation at Scale approach, and our AI-driven and automation tooling, ensures modernisation initiatives deliver optimal return for effort invested, whatever the scale. For more information:

Visit **Amdocs Value-led Modernisation at Scale** or Email at **cloud@amdocs.com** ■

REFERENCES

1. Wakefield Research 2022



Networks demand different security approaches than traditional cybersecurity for IT apps

Dr. Srinivas Bhattiprolu
Nokia

Dr. Srinivas Bhattiprolu (SB), the global head of Pre-Sales and Advanced Consulting Services at Nokia, tells Robin Duke-Woolley, the chief executive of Beecham Research, why IT security and network security must be handled quite differently. Networks truly are critical infrastructure and can be attacked in multiple ways from a vast range of criminals. The challenge for communication service providers (CSPs) in the face of tightening regulation is to ensure they are ready for the threats posed by new technologies

Robin Duke-Woolley: As a quick introduction, can you explain what Nokia now offers for network cybersecurity?

Dr Srinivas Bhattiprolu: We basically have three offerings in the security space. The first one is Security Consulting, which I head up. The second is our range of Security Products and the third is Managed Security Services, where we run the security operations for our customers, who are mainly telcos and CSPs but increasingly also include enterprises, especially those who build critical infrastructure. We basically create security blueprints for our customers which are product agnostic through our security consulting offerings and run the security operations for their network. We do have a threat intelligence lab of our own, where we have close to 50 people researching regularly on various new malwares that are coming into CSPs. We also invest in working closely with standards bodies like NIST through centres of excellence. ▶

SPONSORED INTERVIEW

There are fewer regulations on the IT side, covering areas like data privacy

RD-W: How would you describe the current cybersecurity threat landscape?

SB: One aspect that is very important for us to note is that it is evolving. Secondly, the cybersecurity landscape is becoming more and more complex. When I say evolving, we see a set of new technologies coming into play, new types of threat vectors and actors coming into play, new tools coming into play. According to research from **TM Forum**, mitigating risks arising from the cyber threat landscape is a key factor and accounts for 35% of CSPs' security strategies.

The second point is its increasing complexity, which is evident in three areas:

- There are basically 18 areas in cybersecurity technology, starting with governance and compliance, to device management, to firewalls, to network security, and others to work with. These are different areas with different support requirements.
- Also, there are now close to 2,500 market players, including small startups, medium sized providers and so on. It is very fragmented.
- In addition, new technologies are mushrooming, which means new players are coming in and promising that they can clear these threats. No one player has all the skills, neither large product companies that encompass the world nor smaller companies with specific expertise.

Thirdly, the regulatory requirements are becoming a lot more stringent as countries realise how important critical network infrastructure is. Telco infrastructure is certainly critical infrastructure, so countries are increasingly coming up with cybersecurity plans. For example, the US Executive Order 14028 was passed by Joe Biden in 2021. This talks about cybersecurity and its importance to critical sectors and there are many other countries now, each with their own priorities. The same is the case with UK Telecoms Security Requirements (TSRs) which are supposed to be implemented by all CSPs in United Kingdom.

RD-W: What would you see as the most significant cybersecurity threats that organisations are facing today and how have they evolved?

SB: Regarding cyber threats, lack of cyber hygiene is one of the key areas, then ransomware, then social engineering where phishing plays a part. There are also supply chain risks that cause data breaches and cyber espionage driven by several state and non-state actors. These are the just some of the key threats, and they will continue to be. As we move forward, the threats will continue to evolve, but what is important to us is new technologies and how they are being utilised to really enrich these threat vectors. We as people who are basically protecting security critical infrastructure, have access to the new technologies, but so do the hackers. Today, with US$50 you can actually download a software code from the dark web which will help you launch a DDoS attack. You can download new malware by paying money, so you don't really need to create anything, all you need is to know where these kinds of malwares can be downloaded.

These are some of the things that are there now and are a big area of concern for security practitioners. We uncovered in the 2023 **Nokia** Threat Intelligence Report that the number of IoT devices (bots) engaged in botnet-driven DDoS attacks rose from around 200,000 a year ago to approximately one million devices, generating more than 40% of all DDoS traffic today. An area of great importance – the part I would really like to emphasise – is the lack of skills in cybersecurity. I think that is the biggest challenge we face. Although the situation has certainly improved recently, there are no specific courses in academia. There are a lot less people picking up cybersecurity than we need to work in this area. When you talk about critical infrastructure security where one needs cybersecurity and network skills, this issue is further accentuated.

Also, new threats are evolving, for example, quantum security, which is something that is going to emerge. This will mean that what worked yesterday is not going to work tomorrow. We think that encryption is very foolproof and not going to change, but the whole concept of quantum security means that you are bringing in huge amounts of computing power, which has the capability to break the keys for encryption which are considered to be very robust today. This is a big threat for all the data that is getting stored – how do you change your existing encryption to be quantum safe? How do you change your existing tools to be quantum safe? That is one of the major evolutions that we see.

RD-W: Do you see differences between cyber support needed for IT and cyber support needed for networks?

SB: The first thing is if you are looking at IT, you are basically examining IP traffic. IP packets moving from one application to another. If you talk about the network traffic, it is a lot more diverse and complex. Also, most IT applications are very mature. They are cloud native, basically containerised, so applications are mature. Come to the network, you have physical network functions, virtual network functions, cloud native network functions. It's a combination of these three. The environment is a lot more diverse. Examining the diverse network traffic is a lot more complex than examining only IP packets.

Then there are the tools. The tools that are applicable in the IT space are different. For IT you have identity and access management which are ▶

fairly straightforward. In a network, because there is a lot of legacy, you have to have an interface for command lines to access those network functions. Command line interfaces are not something that exist in the IT space today. The next thing is the concept of APIs. APIs in networks are quite complex today. It's not something that has been very popular, whereas on the IT side integration utilising APIs is very popular and these have been in play for quite some time. Whether this is identity and access management, certificate management or traditional security and event management (SIEM) systems. A traditional SIEM system doesn't need any network-specific context for you to build it, whereas if you deploy the same system on the network side, if it doesn't understand the overall nuances of the network – which is extremely complex and diverse – you cannot really get any insights from it. All you can get is basic data like who has logged into the system. But this total view is becoming a lot more critical for network security operations compared with IT.

The next part is the security operations centre (SOC). The majority of CSPs are separating the network SOC from the traditional IT SOC, so this is becoming very important.

Last but not least are the regulatory requirements. There are fewer regulations on the IT side, covering areas like data privacy. On the network side, they are evolving and becoming more complex. With 5G they are becoming more country-specific, rather than global on the IT side. We are advocating that the traditional ways and means of protecting IT applications won't cut it when it comes to the network and network functions. Operators need to look at a different architecture, different tools and different processes to protect the critical network infrastructure.

RD-W: You talked about country-specific regulations. Can you give some examples of these?

SB: For example, ANSSI has come up with 5G security regulations which are going to be very specific to France. TSRs put forward by the UK are very specific regulations for the UK. These are specific regulations for network service providers. On top of this we have General Data Protection Regulation (GDPR) but that was basically data protection. Then there are other countries with specific regulations such as Germany. In the US we have EO14028. The same is being done in Australia. Japan is trying to do the same. China and India also. Certification is becoming very important, and we see this in India, Singapore and many others. In Singapore, telcos require that all the products in their infrastructure must be NESAS certified. India is bringing out something called an India Telecom Security Assurance Requirements (ITSAR) regulation. If your products do not meet the ITSAR regulation, then they cannot be deployed by Indian CSPs.

The biggest change is the amount of penalties. For example, UK telecoms TSR proposes 10% of the turnover as a penalty or £100,000 per day, which will essentially mean they will wipe out the entire operating profit of a telco if they don't comply with the requirements and experience a breach/attack. All are talking about the punitive measures the telcos will have to pay.

So that's where the difference is. The regulations are becoming a lot more stringent, and a lot more inclusive when it comes to the telecom infrastructure. We see a lot more certifications coming into play. We see more rules for vendors like us playing a part in initiatives like the Network Equipment Security Assurance Scheme (NESAS) brought in by 3GPP and GSMA. That's not going to be enough. Regulators are continually asking the CSPs to prove that their network infrastructure is secure. What proactive measures they are taking to prevent any state actors or rogue actors from gaining access to their networks. So that is being asked and 5G is adding extra complexity here. ▶

> We are advocating that the traditional ways and means of protecting IT applications won't cut it when it comes to the network and network functions

The regulations are becoming a lot more stringent, and a lot more inclusive when it comes to the telecom infrastructure

RD-W: Why are the penalties so high? It sounds like, if you get it wrong, we'll bankrupt you.

SB: You have to think of the consequences. Take something that happened quite recently. There was a multi-level attack on a national network which happened through traditional social engineering meaning someone accessed the network. They understood how the network is structured in terms of topology. They erased the backups. The result was the network went down. Then what happened – the post offices could not function. Hospitals could not function. Transport and industry came to a standstill. The entire critical infrastructure within the country pretty much came to a standstill. In other words, it's not just the telecoms provider that gets affected, there is a major effect on everything. You can basically bring an entire country to a standstill for a period of 48 hours or so. Utilities can be affected. Transportation can be affected. So that's something no government can afford to ignore. That is the reason they are attaching huge importance to the networks as critical infrastructure.

RD-W: It's an incentive to make sure that they have sufficient expertise looking at it to make sure these things don't happen.

SB: Absolutely. It is basically creating a need for making the investment into processes within security that will proactively prevent these attacks and make their network infrastructure a lot more resilient. Telecoms networks are definitely critical infrastructure. It can bring down countries.

RDW: How do automation and analytics work together to strengthen cybersecurity defences?

SB: Analytics gives you the right visibility, for example, taking one of our own products at Nokia where we are utilising machine learning algorithms to scan the network functions on a regular basis. We provide a digital twin of the network and then we scan the network functions to assess if any spurious traffic is going across. We build a real time threat index for each network function. So that is very important. The proliferation of AI/ML into the protective mechanisms, the signatures and detecting malware, preventing social engineering and all that – that is happening.

In terms of automation, it is very critical because firstly there is certainly a reduction in capex and opex so operators cannot invest in people even if they want to. There are not enough experts available, so a major way forward is automation. They are looking for a single pane of glass. They are looking for automated actions, semi-automated actions and workflows. How they can build tools on the network that can detect specific issues and then take automated/semi-automated actions in order to reduce, if possible, the manual interventions. Automation is playing a very critical role in the entire security area, and so is AI/ML.

According to a recent survey by TM Forum, 51% of CSPs agree that they require an automated response to threats. Together, I believe AI and automation can aggregate analysed data from multiple vendor systems. You can define automated responses to really look at threats and I think that's something we can do.

RD-W: You talked earlier on about the skills gap. Are you saying that there is a need for more automation to cater for that? How do you deal with the skills gap?

SB: I read an article recently which said that by 2025 our industry will have a shortage of close to 3.5 million qualified professionals in security and cybersecurity. It doesn't matter if that's enterprise or network but 3.5 million overall is a huge gap.

Certainly, governments need to take steps for new certification plans to launch new courses in cybersecurity. There is a clear need among the entire community to encourage more students and people from other industries to take up security as their career path.

Automation can address this problem to a certain extent but it cannot help you completely. Having qualified experts is extremely important so we have to work on both sides: the repetitive tasks can be managed through automation and the job of experts can be made a lot easier by having automation and having functionality like a single pane of glass. You cannot overstate the importance of having the right level of expertise because all of these automations, principles and solutions are going to be defined by these experts. So, it is a difficult situation where you have a gap in the number of security experts. The entire ecosystem of players, which includes government, academia and industries, has to come together to make sure that they are attracting more numbers of people from different age groups and backgrounds into the security industry.

RDW: What are the key take-aways from what you have been saying?

SB: The most important point is IT versus network. The traditional approach of utilising tools and protecting IT applications is not going to work when it comes to networks. That is the key message. Traditional IT tools for identity and access management, and certificate management are not appropriate for the network side. This is very important.

I see many people now showing interest and subscribing to this particular view. IT and networks are different and it is increasingly evident that it is necessary to have network-specific tools for securing critical infrastructure.

Networks are a lot more diverse than IT and having the right protection mechanisms in place is crucial.

Next are the regulatory changes. 5G has brought a lot more complexity into the network. Securing networks has become a lot more complex. It is a job for security experts with a detailed understanding of network technologies.

The divergence between IT and networks in the security space is large and will become a lot larger as the cyber threats and regulatory requirements develop further. ■

ANALYST REPORT

How will telco networks manage cybersecurity as the threat surface expands?

SPONSORED BY

NOKIA

What role do telco networks have in the threat landscape?

According to IBM's Cost of a Data Breach Report 2023, the global average cost of a data breach in 2023 was US$4.45m, a 15% increase over three years. Cybersecurity is more important now than ever before, and malicious actors have grown far more savvy in recent years, writes Robin Duke-Woolley, the chief executive of Beecham Research. What are the implications for telco networks over the next few years? ▶

Estimated cost of cybercrime worldwide (in trillion US dollars)

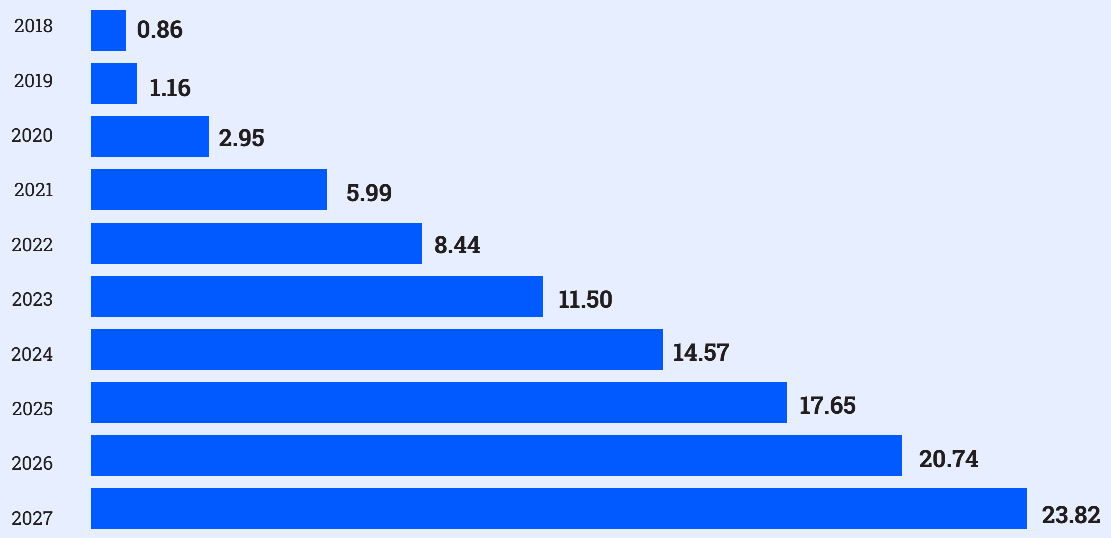


Figure 1: Estimated growing cost of cybercrime 2018-27

Source: Statista, National Cybersecurity orgs

It has been said that cyber theft is the fastest growing crime in the United States by far. **Figure 1** is an estimate of the cost of cybercrime worldwide. What this highlights is that the cost of cybercrime is enormous and growing quickly.

Nokia's Threat Intelligence Report 2023 highlights the following key points regarding the cyber threat landscape:

Regarding mobile networks:

- Communications service providers (CSPs) are struggling to keep up with the latest threats. More than 30% of CSP respondents to a Nokia/GlobalData survey said they had experienced eight or more breaches in the last 12 months.
- More than half of the CSP respondents said fragmented tools make it difficult to effectively implement security capabilities across various systems and use cases.
- CSPs are carefully considering geopolitical developments when evaluating and mitigating security risks.

Regarding malware attacks:

- In total, 35% of the malware attacks detected were either ad-click bots, crypto-miners or banking trojans.
- While adware decreased by 25%, crypto-mining kept stable and banking trojans almost doubled, climbing from 5% in 2021 to 9% in 2023.
- Residential malware infection rates continue to decline, falling from 3% to 1.5% — but still remain above the pre-pandemic rates of 1%.

Regarding DDoS attacks:

- The rise of IoT and cloud technologies in both residential and enterprise networks has contributed significantly to the expansion of botnets.
- Botnets have become a major generator of DDoS traffic. Between 500,000 and 1,000,000 globally distributed, remotely controlled IoT hosts or cloud server instances are active daily, generating more than 40% of all DDoS traffic.
- In 2023, 90% of complex, multi-vector DDoS attacks were based on botnets.

These findings indicate that the cyber threat landscape is becoming more complex and more diverse. The presence of state actors, associated with geopolitical developments, is also now a major factor. ▶

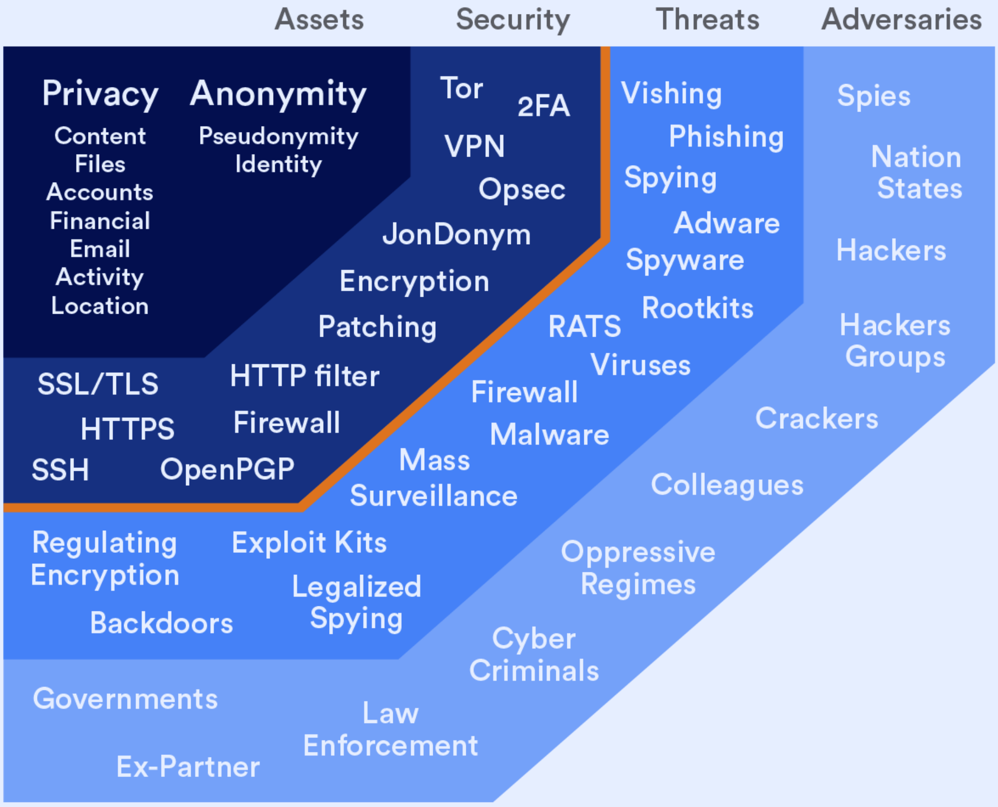


Figure 2: The cybersecurity challenge – protecting assets from threats and adversaries

Growing threat complexity

The following quotes give an idea of the growing complexity of the threat landscape:

- "Cybersecurity experts have another word for hybrid workplaces: Nightmare. The hybrid workplace, they say, is fertile ground for would-be hackers and other malicious actors," Wall Street Journal
- "Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances and other devices attached to the Internet," information security expert Dorothy Denning

Figure 2 illustrates the growing set of challenges facing cybersecurity. The number of potential adversaries is increasing and is not limited to traditional hackers. As a result, threats are evolving in complexity.

Telco networks as critical infrastructure

The telco industry contributes typically around 4-5% of a country's gross domestic product (GDP) and might therefore be considered of relatively minor importance to the country. However, its own GDP does not reflect the wider importance that telco networks play in the economic and social wellbeing of the country. Almost every business is dependent on telco networks to transact business, as is every branch of central and local government and related public bodies.

The social life of the country is highly dependent on telco networks as well, for example the capability to broadcast TV to every home, for friends to text one another to arrange their appointments or for anyone to summon emergency services via an emergency phone number. The defence and security of the country is also highly dependent on reliable communications. Telco networks therefore have a multiplier effect and their importance to the overall continuity of life in the country is enormous. Such is their importance that governments have recognised that the issue often transcends the narrower commercial interests of the companies who supply services. Governments clearly have a duty to ensure the resilience of their country's telco networks and services.

The importance of telco network resilience is reflected in the fact that many governments have identified telecommunications as one of the top 10 sectors deemed to be part of the critical national infrastructure (CNI). The UK government for example ▶

views the CNI as those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could:

- cause large scale loss of life
- have a serious impact on the national economy
- have other grave social consequences for the community
- be of immediate concern to the national government

Telco networks fit with each of these four points. As a result, governments have enacted increasingly stringent requirements for security of their countries' telco networks and high penalties if those requirements are not met.

At the same time, telco networks present a complex architectural and infrastructural landscape to secure. From distributed and cloud radio access networks (RAN), edge and cloud core, enterprise and subscriber devices, gateways, hubs, set-top boxes, multi capacity routers, switches, base transceiver stations, femtocells, and 5G edge gateways, there is significant diversity and complexity that telcos have to deal with when it comes to cybersecurity.

Since telco networks are communication enablers, they get attacked often as they are on the radar of hacker groups, advanced persistent threat (APT) groups and clusters, malicious actors and malware developers. Telcos can be targeted in two ways. Their infrastructure can be used to launch large-scale attacks on third parties or telcos and their infrastructure could themselves be targeted.

The rapid expansion of threat surfaces and digital infrastructure associated with telcos has led to a sudden and rapid increase in the number of threat vectors that are growing in complexity, scale and sophistication.

The impact of new technologies

New technologies have the potential of responding to new cyber threats more quickly and more efficiently, particularly at scale. In the hands of bad actors, some are also being used to create new threats. The following are some of the latest technologies having most impact on cybersecurity:

- **Artificial intelligence (AI) and machine learning (ML):** Artificial intelligence and machine learning are having a major impact on the cybersecurity industry. These technologies analyse huge amounts of data, learn from patterns and make predictions about potential threats. By utilising these technologies, cybersecurity experts can automate the identification and response to threats faster and more accurately than ever before.

- **Behavioural biometrics:** Behavioural biometrics is a new approach to cybersecurity that uses machine learning algorithms to analyse user behaviour. This technology can detect patterns in the way users interact with devices, such as typing speed, mouse movement and navigation. By analysing these patterns, behavioural biometrics can identify potential threats, such as hackers who have gained access to a user's account.

- **Zero trust architecture:** Zero trust is a security model that requires strict identity verification for every person or device that tries to access an organisation's network or resources. This model assumes that no one is trusted by default, even if they are within the organisation's network perimeter. Zero trust architecture has gained popularity in recent years due to the increasing number of cyberattacks targeting businesses and organisations.

- **Quantum computing:** Quantum computing is a technology that uses quantum mechanics to process data. It has the potential to solve complex problems much faster than traditional computers. While this technology is still in its infancy, it has the potential to revolutionise the field of cybersecurity by allowing more secure encryption.

- **Cloud security:** Cloud computing has become an essential part of many businesses, but it also introduces new security risks. Cloud security technologies are emerging to address these risks, such as multi-factor authentication, encryption, and access controls. By utilising these technologies, businesses can ensure that their data is secure in the cloud.

Regarding the impact of these, a major one relates to quantum computing. This is all about having very large amounts of computing power. This is at an ▶

early research stage by academia and by product vendors at present but once in the market it will have the ability to break the encryption codes of today. As a result, new types of encryption technologies are likely to emerge which will be quantum based. But this will present new challenges – how do you improve the existing data that has already been encrypted and how do you deploy that?

A further area is AI, which can be a threat as well as an opportunity. Bad actors are utilising AI to build sophisticated threats while those who are the protectors are using it to build sophisticated protections. The technology is available for both the hunter and the hunted. As a result, evolution and having models that learn over time will be very important, but it will be necessary to continuously monitor and continuously train models so they do not become obsolete. Essentially, what works today cannot be assumed to work tomorrow. The threat landscape will constantly change.

The skills gap

In addition to these threats and rapid technology evolution, the skills gap is a major issue for implementing cybersecurity. To take the example of just one country, the UK government issued a statement in July 2023 that included the following observations:

- 50% of all UK businesses have a basic cyber security skills gap, while 33% have an advanced cybersecurity skills gap. These figures are similar to 2022 and 2021.
- There were 160,035 cybersecurity job postings in the last year. This is an increase of 30% on the previous year. 37% of vacancies were reported as hard-to-fill (down from 44% in 2022, but same as 2021).
- There is an estimated shortfall of 11,200 people to meet the demand of the cyber workforce (down from 14,100 last year, largely due to slower growth of the sector).

These issues are apparent in many countries. ISC2 is the world's leading member association for cybersecurity professionals. Its statement on the skills gap for 2023 is as follows:

"In 2023, our research calculated that the global [cybersecurity] workforce grew to an all-time high of 5.5 million, an increase of 440,000 jobs compared to 2022, a rise of 8.7%. For comparison, in 2019 the global workforce was estimated at 2.8 million. At the time, this was seen as an impressive figure and yet the workforce has continued to expand rapidly ever since, despite encountering obstacles such as the COVID-19 pandemic and economic challenges across the globe. This is good news and should be celebrated, yet it remains in the shadow of unfulfilled demand. In 2022, the gap between supply and demand was estimated at 3.4 million; a year later this reached four million. This leaves the profession struggling with the seeming paradox that it is employing an ever-greater number of people in cybersecurity roles but at a pace that never quite catches up with the underlying need in terms of numbers or specific skills."

ISC2's message is that the cybersecurity workforce must double in order to adequately protect organisations and their critical assets.

Nokia cybersecurity offerings

In response to these challenges, Nokia has three offerings in the cybersecurity space:

1. Security Consulting

Nokia Security Consulting brings deep 5G security expertise and one of the world's only end-to-end 5G security assessment and insight capabilities to help CSPs transform their 5G security operations and stay ahead of cybersecurity threats. The company has the in-house expertise to manage cyber threats and protect the security and privacy of sensitive business data, critical infrastructure, and all other aspects of critical networks.

The company offers 5G security concepts and designs for 5G packet core, Voice-over-Next-Radio, SDL or OpenRAN and then advise on the matching security operations governance and SOAR use-cases. Having a consolidated view of security threats and security posture, CSPs can detect, respond to and recover from security breaches faster.

2. Security Products

Designed with real-world applications in mind, Nokia's end-to-end security products portfolio includes use-case driven technologies and are effective at blocking threats in security operations centres such as:

1. Nokia's telco-XDR Security Operations suite NetGuard Cybersecurity Dome
2. NetGuard Endpoint Detection and Response
3. NetGuard Identity Access Manager
4. NetGuard Audit Compliance Manager
5. NetGuard Certificate and Automated Lifecycle Manager

While traditional IT security products are more generalised and focus on a broader range of digital assets, telco network security requires specialised expertise and solutions as it demands ▶

compliance with strict regulatory standards that vary from country to country and are specific to the telecommunications industry.

3. Managed Security Services

Nokia Managed Security Services offers the most complete portfolio of value-added telco security services tailored to protect both OT/5G networks and IT technology from the evolving cyber threats in the 5G and Industry 4.0 era:

- Security Risk Index (SRI)
- Security Infrastructure Management (SIM)
- Security Governance, Risk and Compliance Management (GRC)
- Managed Detection and Response (MDR)

Nokia's Managed Security Services portfolio is fully aligned with the 'Continuous & Defense-in-depth Adaptive Security Architecture', as well as references including MITRE ATT&CK, Nokia's Bhadra Telecom Framework, and ITU-T x.805. ■

Click for more information on Nokia cybersecurity offerings

Case study

Nokia's Security Operations Platform, NetGuard Cybersecurity Dome, seamlessly integrates cutting-edge GenAI/LLM technology, revolutionising operational efficiency across different phases. In the detection phase, GenAI assists in Threat Hunting, empowering analysts to swiftly uncover potential threats. The Resolution phase benefits from accelerated Incident Triage as language models facilitate rapid synthesis and interpretation of vast information. Additionally, in the forensics phase crucial for audit and compliance, GenAI contributes to comprehensive analysis during incident reviews, ensuring scrutiny by external auditors.

NetGuard Cybersecurity Dome, an award-winning solution, harmoniously combines security modules like EDR, privileged access management, audit compliance, and threat intelligence. This interconnected ecosystem ensures that collective intelligence exceeds individual components, providing security analysts with enriched insights from real-time data sources. Going beyond read-only capabilities, our telco-centric large language models (LLM) can be configured to propose actions such as creating detection rules, configuring extract, transform, and load (ETL) processes, and running playbooks, all guided by SOC analysts.

In a recent real-world scenario, our customers are going to utilise our LLM integration through a series of interactions, specific queries, and requests for relevant information.

Nokia's telco-centric trained intelligence system promptly correlated data from various security controls and log analyses. This method gradually unveiled critical details about a suspicious workload deployed on the 5G core, RAN or transport network, showcasing the effectiveness of our AI-driven investigative approach in security operations for service provider and critical infrastructure enterprises.

Nokia will introduce and demonstrate multiple telco-centric GenAI use cases for security operations during Mobile World Congress in Barcelona from 26-29 February 2024.

Click here to learn more about Nokia's security offerings.

NOKIA

About Nokia

At Nokia, we create technology that helps the world act together. As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry. Leading in critical network security transformations, we play a key role in establishing security standards with five standardisation bodies. With 15+ years of in-house security experience and 200+ telecom-specific use cases, we support 500+ customers worldwide.

Future first - Experience the power of connection at MWC Barcelona 2024

MWC Barcelona 2024 is once again shaping up to be the place to connect with the world's most influential leaders and thinkers, catch up on the latest digital trends, discover the game-changing power of mobile technology and access world-class content. Hosted by the GSMA at the Fira Gran Via in Barcelona from 26 – 29 February 2024, registration is open

You will not want to miss the event's diverse line-up of keynote speakers which includes industry giants, technology pioneers and thought leaders, so secure your pass to the world's largest and most influential connectivity event now.

Speakers include **Alef Aeronautics** CEO, Jim Dukhovny, who will share his experience designing and developing flying cars; **Dell Technologies** founder, chairman and CEO, Michael Dell, who will talk about the importance of Dell being a valued partner for telcos; **Ethiopia Telecom**'s CEO Frehiwot Tamiru will share her technology vision for telcos across Africa; **Oxford Quantum Circuit**'s CEO, Ilana Wisby who will discuss all things Quantum-as-a-Service; **Microsoft**'s vice president and chairman, Brad Smith; **Xtend**'s co-founder and CEO, Aviv Shapira, showcasing how 5G mobile technology is the catalyst for robotics.

All discussions at MWC Barcelona will be centred around the event theme, Future First, which speaks to the urgency of bringing industries, continents, technologies and communities together to realise the future's potential. The agenda will be shaped by six sub-themes reflecting the latest trends and technologies. These themes will feature across the 17 different stages we have across the nine halls of MWC and 4YFN, providing a platform for over 1,100 speakers. The themes are 5G and Beyond, Connecting Everything, Humanising AI, Manufacturing DX, Game Changers, Our Digital DNA.

2024 is a special year as we will celebrate the tenth edition of 4YFN, the global digital and tech startup event which partners with MWC to showcase global tech entrepreneurs and the business leaders of the future. Over ten years, 4YFN has helped startups thrive, starting with exposure to investors and the business community at MWC and continuing throughout the year with the online 4YFN global community of founders and investors.

Taking place across Halls 8.0 and 8.1, 4YFN will welcome some of the hottest names in the global startup scene including Sir Martin Sorrell, founder and executive chairman at S4 Capital and ▶

Nigel Toon, CEO, chairman and co-founder at **Graphcore**. The 4YFN agenda will feature trailblazing talks and debates, with discussions centred around the 4YFN themes: the Age of AI, Growth, Startup Funding, Corporate Innovation, Art of Innovation and Decentralisation and Beyond.

Unleash digital transformation across industry and society

MWC Barcelona has long provided a forum to showcase how connected technologies are transforming the mobile industry, but the event's reach now stretches far beyond, reflecting the impact of mobile on vertical business sectors. MWC celebrates the broader ecosystem of players across adjacent industries who are central to digital transformation. Over half of attendees to MWC are from businesses beyond the mobile industry, and every year the event is more vertically diverse. Building on this, the organisers are enhancing focused areas to convene the decision-makers and thought leaders who are accelerating the next wave of digital transformation across the entire connectivity ecosystem.

MWC is where leaders gather to get deals done which is why it is a pivotal moment in business calendars, year after year. With this in mind, a hub in Hall 6 is being created that is dedicated to bringing leaders together across a range of collaborative networking areas, auditoriums and a VIP lounge. Combining networking and innovation, Hall 6 is shaping up to be a hot spot of inspiration and must-attend immersive experiences with the return of Journey to the Future, MWC's high-tech feature area. It will showcase game-changing innovations with technology's transformational impact on tomorrow's industries, communities and citizens.

Elsewhere, Hall 4 will feature the Connected Industries space which invites attendees to discover how mobile technologies are changing the face of four spotlight industries – manufacturing, smart mobility, fintech and mobile commerce and sports and entertainment. Global industry experts will take to the Connected Industries stage across each of the four days at MWC Barcelona, exploring topics such as the commercialisation of drones, the emergence of robots in smart factories, the future fraud landscape and the role of technology in creating world-class fan experiences.

MWC Barcelona will also once again be co-located with Sports Tomorrow Congress, presented by the Barça Innovation Hub (BIHUB). Sports Tomorrow Congress is a showcase of the decades of knowledge that FC Barcelona has accumulated on topics such as health, nutrition, high athletic performance, the digital sphere, and all topics related to sports and their impact on society.

Across Halls 5, 6 and 7, Pavilions from around the world offer delegates the chance to network with country trade bodies, policymakers and digital hubs. MWC Barcelona is the place to network, make new connections and catch up on the latest digital trends, with the largest gathering of policymakers who enable the digital economy, brought together by the GSMA Ministerial Programme. Ministers, heads of regulatory authorities and policymakers come to MWC every year to meet with mobile industry CEOs and senior representatives of international organisations, share knowledge, and evolve priority policy and regulatory issues. ■

Over ten years, 4YFN has helped startups thrive

protecting the digital identity of consumers and businesses

convenience
and simplicity
that consumers
demand

IDENTIFICATION
VERIFIER

iconectiv