european
COMMUNICATIONS

THE LAST WORD ON NETWORK OPERATOR STRATEGY FROM AROUND EUROPE

Q4 2017 ISSUE
www.eurocomms.com
@eurocomms

Mobileum:

Jaskaran Singh, Head of Data Science, talks about bringing AI to a number of real-world telco use cases

MOBILEUM SPECIAL PROMOTION

Helping propel your network to the next generation

The speed of technological developments demand test solutions to continually evolve.

We enable our customers to analyse, develop and validate the performance and capability of a wide variety of network functions and devices, providing improved operational efficiency and security.

By continuing to innovate, we ensure you stay ahead of market need, empowering you to prove network performance under real-life usage conditions before the availability of actual device hardware.

Our TM500™ is the industry standard network test platform, used by all the major infrastructure vendors worldwide to validate their networks.

Our TeraVM® is a virtualised application emulation and security performance test solution, ensuring that highly optimised networks and services can be delivered with minimal risk.

Visit Cobham Wireless at MWC 2018, Hall 6 Stand D50!

www.cobhamwireless.com/mwc2018

COBHAM

Contents

11 Tele2 Group CEO: From value for money connectivity to being an IoT titan
Tele2 is a past master among challenger brands, with reputation for market-challenging ideas, as well as commercial propositions

european
COMMUNICATIONS

Cyber security, CMOs and price conscious consumers

Conceived wisdom dictates that digital native companies are the benchmark that telcos need to measure themselves against when it comes to anything from services and customer experience to security. So news in November that one of the poster children, Uber, had not only suffered a data breach involving 57 million customers and drivers but had also decided to cover it up, would have no doubt raised a wry smile in telco boardrooms around the world.

Keeping customers and data safe is hard. It is becoming increasingly more challenging, however digital your business is, so it is timely that we make security the subject of our latest special report. Our survey shows that the telecoms industry thinks it is doing a decent job amid increasing hacking attempts, and that the necessary improvements they know they need to make are more cultural than technological in nature.

Reflecting the double-edge sword of security, we speak to Deutsche Telekom's Vice President of Cyber Defence Response about the incident that saw 900,000 routers go offline this time last year and assess how telcos can succeed in selling security services to the enterprise market.

A security breach is something that is likely to keep telco marketers up at night. European Communications delved into all things marketing at our annual CMO roundtable in October. We provide the choice cuts this issue, including the view of Three UK's Tom Malleschitz, speaking about the industry as a whole: "We are ripping customers off all the time. We lure them with cheap deals, cheap monthly fees, then you go over your allowance [and] we don't tell you."

This issue's C-suite section features a more circumspect Tele2 Group CEO Allison Kirkby. The exec discusses her ongoing battle to "sustain a competitive advantage in our cost structure, so that we can continue to offer great value for money connectivity". With consumers not wanting to pay much for it, Kirkby says the operator is looking elsewhere. "Tele2 IoT is on a journey to become a titan in the IoT space," she says.

In short then, this issue is a microcosm of the opportunities and challenges that the industry is facing as 2017 draws to a close. Have a great Christmas and a happy new year.

Marc Smith
Editor

SJP business media

Professionals based in the UK and Europe can apply for a free subscription to European Communications at www.eurocomms.com/register

Subscription prices:
UK £65
Overseas £90

Follow us on Twitter @eurocomms

Join us on LinkedIn

Editor
Marc Smith
marc.smith@eurocomms.com
T: +44 (0) 207 933 8999
Twitter: @eurocomms

Staff Writer: Alex Sword
alexs@eurocomms.com
T: +44 (0) 207 933 8999

Publisher
Wayne Darroch
WayneD@sjpbusinessmedia.com
T: +44 (0) 207 933 8999

Design and Production: Alex Gold

Account Director: Fidi Neophytou
fidin@sjpbusinessmedia.com
Tel: +44 (0) 207 933 8979

Account Manager: Richard Baker
richardb@sjpbusinessmedia.com
Tel: +44 (0) 207 933 8979

Subscriptions/Circulation
SJP Business Media
Unit K, Venture House
Bone Lane
Newbury
RG14 5SH

T: +44 (0) 1635 879361
F: +44 (0) 1635 868594
E: europeancomms@circdata.com
W: eurocomms.com

SJP Business Media
(ISSN 1367 9996) All Rights Reserved.
No portion of this magazine may be reproduced without written consent.
The opinions expressed are not necessarily those of the publisher, who accepts no liability of any nature arising out of or in connection with the contents of this magazine.

European Communications is published quarterly by:
SJP Business Media,
52-54 Gracechurch Street
London, EC3V 0EH

From East to West we keep you in touch

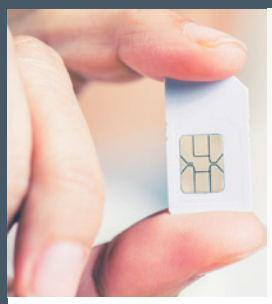
We are based in Cyprus, at the crossroads of Europe, Asia and Africa. Through our state-of-the-art global network, we provide a wide range of international telecommunications products, services and total solutions, making Cyprus a major telecommunications hub in the Eastern Mediterranean and a telecommunications bridge between East and West.

- Submarine cable capacity
- Satellite turnaround services and Teleport facilities
- Dedicated fiber links to major international POPs
- Ethernet & MPLS-VPN connections & private leased lines
- Global internet connectivity
- Premium quality international wholesale telephony

From East to West
we keep you in touch

cytaglobal

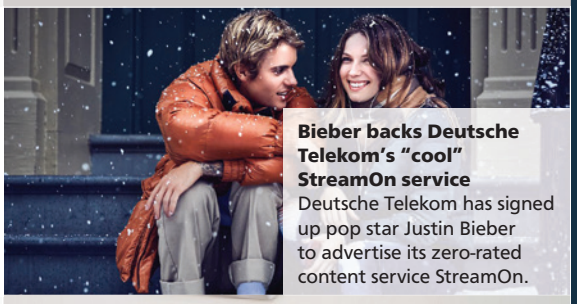
Get all the latest news about telecoms in Europe at www.eurocomms.com



Operators warned as SIM-only contracts become most popular mobile tariff in the UK
UK consumers bought more SIM-only contracts than PAYG or traditional post-pay methods including a device in the third quarter, leading to warnings that operators need to re-evaluate their business models.

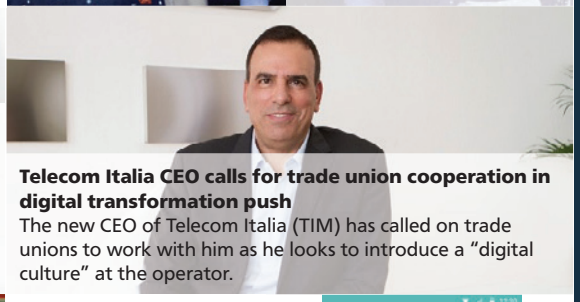
Deutsche Telekom brings Netflix to all opcos with new deal
Deutsche Telekom has extended a deal with Netflix to make content from the Stranger Things producer available to all of its subsidiaries in Europe.

Vodafone IoT division wins telematics deal with UK car insurer
Vodafone is providing telematics technology to support a usage-based insurance offering from UK company Admiral.



Bieber backs Deutsche Telekom's "cool" StreamOn service
Deutsche Telekom has signed up pop star Justin Bieber to advertise its zero-rated content service StreamOn.

Liberty teams up with merchant bank to target SMEs in the UK
Liberty Global is launching an enterprise-focused joint venture in the UK with MXC Capital.



Telecom Italia CEO calls for trade union cooperation in digital transformation push
The new CEO of Telecom Italia (TIM) has called on trade unions to work with him as he looks to introduce a "digital culture" at the operator.

Telefónica looks to start-up talent for innovation arm
Telefónica has tapped its 2015 investment CARTO for the new head for its entrepreneurship division.

Telefónica enables offline social media use with new Pigram app
Telefónica has found a novel use for text messages with a new service that allows subscribers to use their social media accounts when data services are not available.

T-Systems acquires SAP specialist in Hungary
Deutsche Telekom's enterprise arm has acquired Hungarian company ITgen as it looks to boost its offering to businesses in the central European country.

Altice moves to reassure markets on debt, expects disposals early 2018
Altice has moved to clarify what it said was "misinformation" and reassure the financial markets about the strength of the company's balance sheet.

Opinion

Under-The-Top disruption has arrived, but it doesn't have to be a threat to telcos
By Bengt Nordstrom, Co-Founder and CEO of independent telecoms business consultancy Northstream

Q&A

Nick Jeffery took the reins of Vodafone UK in September 2016. He talks about his first year in charge and why he hopes competitors will fear the company moving forward

Analysis

Movistar+ seeks to balance content risks with commercial reality
Just a couple of years ago Telefónica was happily aggregating content from traditional sources to entertain subscribers in its home market, but in January this year that all changed.

Discover the latest developments from Europe's telecoms space with our free daily newsletter

Register today for European Communications' daily e-newsletter and keep pace with the key events in the telecoms industry. Alongside all the latest news, you can read exclusive analysis, opinion features, Q&As with industry thought leaders and white papers to download.

www.eurocomms.com/newsletter

Key trends we cover include:

Financial/M&A
Regulation
Back office/IT
IoT
Big Data
Customer Experience
Fibre Broadband
Enterprise

@eurocomms

/eurocomms

European Communications

French telecoms market

Five years ago, France was rocked by the arrival of low-cost entrant Free Mobile. It has now taken almost 19 percent of the mobile market and is rapidly catching up on Bouygues Telecoms. Orange remains the number one player across broadband, mobile and TV, while Altice-owned SFR has suffered more subscriber losses than its rivals over the past 12 months

Mobile: **31.62 million** (+2.12 million)

Broadband: **11.4 million** (+346,000)

TV: **6.84 million** (+329,000)

Mobile: **20.3 million** (-400,000)

Broadband: **5.83 million** (-172,000)

TV: **4.24 million** (+82,000)

Mobile: **13.94 million** (+1.28 million)

Broadband: **3.34 million** (+341,000)

TV: **not disclosed**

Mobile: **13.39 million** (+1.01 million)

Broadband: **6.49 million** (+168,000)

TV: **not disclosed**

Figures, which show customer numbers, are correct as of 30 September 2017. Year-on-year increase/decrease shown in brackets.

Mobileum: AI-enabled analytics is a strategic enabler for telcos in a digital world

In a data-hungry digital world, with increasingly diverse mobile connections driven by IoT and 5G networks, there is a critical need for a more cost-effective, digital way of managing the whole telco ecosystem. Artificial Intelligence (AI) is pivotal to this transformation, in combination with other strategic data science investment.

Blending AI analytics with big-data and service delivery platforms, supported by specialist data science and domain expertise, is the key to delivering tangible business impact, says Jaskaran Singh, Senior VP for Big Data & Analytics at Mobileum.

AI has the potential to have a major impact on all aspects of the CSP business. From optimization and automation of the network, to improving customer engagement, to workforce automation there are very few areas where advanced anaytics and AI will not have a role to play. Mobileum uses AI today to analyse and predict customer behaviour on the network, and act on the insight to improve campaign performance, to identify complex network security threats, and to prevent sophisticated usage fraud. In this article Jaskaran Singh explores how AI is transforming the Fraud problem for CSPs.

European Communications: Big-data analytics and AI is a hot topic across many markets at the moment. Where does Mobileum see this kind of advanced data science having the biggest appeal and impact for telcos at the moment?

Jaskaran Singh: AI has great potential, but we focus on the areas where we can deliver the most value. The key to delivering value is the ability to combine domain expertise, data science and the

technology to take actions in a single platform. We deliver solutions based on our Active Intelligence platform which combines all three. Our heritage is in networks and roaming which is like a microcosm of the whole CSP business and we have leveraged that deep undertanding of that domain to deliver new value with AI powered solutions in customer segmentation and targeting, in signalling security and in fraud.

Given all the negative publicity around security breaches in telecoms lately, is analytics being embraced more widely now?

It ought to be, given how rampant threats are now and the potential damage CSPs are risking. In US dollars, global fraud loss is estimated to be costing the industry $29.2 billion annually now, accounting for 1.27 percent of global telecom revenues. Operators could be stemming millions in losses by developing more sophisticated fraud detection and prevention capabilities. If a customer suddenly finds a €500 charge on their bill because their phone has been hijacked, the ramifications are huge. One post to Twitter and confidence in a brand can slide sharply.

What are the costliest issues for operators currently?

Interconnect bypass (for example SIM Box) events are the most common problem, accounting for $4.27 billion, but International Revenue Share Fraud (IRSF) is the costliest issue, adding up to $6.10 billion in losses, according to the Communications Fraud Control Association (CFCA).

The trouble is that fraudsters are experts at avoiding detection, quickly finding new ways round the latest security measures. Legacy systems can't keep up with that. Being rules-based, they're good at spotting and reacting to known issues but not at picking up emerging threats. Also, they're limited by finite databases which at best are likely to be able to hold up to three months' worth of data – that's no use for tracking discrete patterns of potentially fraudulent activity over time. You may need to be able to go back several years to do this.

That's where big data analytics, using AI, neural networks and machine learning, comes in: very high capacity, intelligent systems which are quick

> "The key to delivering value with AI is to combine domain expertise, data science and a platform that can take action in real-time"

to learn what constitutes potentially suspicious activity. By performing very complex analyses, the technology can pick up the subtlest patterns in a vast range of data - to a degree that hasn't previously been possible.

How do traditional fraud detection methods fall short?

It's about having to second-guess what fraud might look like: this is what rules-based systems rely on. You might set the system to generate an alert if more than 60 minutes of usage is incurred by a subscriber after 11pm from a blacklisted cell site, for instance.

Such rules invariably have a very high rate of false positives – greater than 50 percent in some cases. They might for example flag up heavy users on unlimited bundles (service abusers rather than fraudsters), business users, service numbers, telemarketers and so on. This indiscriminate event capture leads to a lot of time being spent by fraud analysts to weed out the false positives, significantly increasing the latency of fraud detection.

And actually instances of fraud tend to be few, yet very high impact. There's little value in picking them up at some point after the fact, as by then most of the loss has already occurred. So operators need to be much more targeted in their efforts, and machine learning-based fraud analytics makes that possible.

Today's detection rules tend to be based on thresholds too but, as fraud evolves, those thresholds are changing so there's a need to monitor new usage attributes in order to detect fraud early.

Isn't there a danger in relying on machine intelligence?

AI's role is to detect the previously undetectable and do it quickly. Operators can still set strict controls and train systems what to look for, what level of sensitivity is appropriate, and what action to take.

It's about making fraud detection more intelligent, targeted, accurate and cost-effective. The 'machine learning' part means systems can be trained – and, even better, train themselves - to distinguish real threats from false positives or 'noise'. So, over a very short period of time, they become highly accurate at telling the difference - only flagging or reacting to scenarios that are genuinely a risk. This improves the hit rate and speed of discovery, and saves fraud analyst teams from wading through reams of false alerts, driving up cost-efficiency.

A carefully implemented AI solution that is continuously adapting, and aids human decision-making when required, can be very effective in reducing fraud significantly.

> "AI-based analytics is the next essential investment in fraud control"

The benefits of this approach seem obvious. So why aren't more operators using this kind of technology in their fraud strategies?

I think fraud managers have been reti-

cent to ask for new budget after promising that their existing systems were the definitive solution to addressing today's growing threats. Also, operators' fraud analysts tend to be finance people, who don't really understand the technology. Ultimately, fraud control is still viewed as a cost centre. It requires boldness and a bit of rebellion to break away from existing approaches, but the growing risks make this an imperative now.

How are you managing to increase the sense of urgency at the companies you talk to?

We try and remove a lot of the barriers to AI adoption by shielding operators from the complexity (the highly sophisticated mathematical algorithms being applied to complex raw data - as held in operational, billing and CRM systems, for instance). Our Active Intelligence platform automates as much as possible, so that as the software discovers events, it can test their irregularity and act without intervention (for example, by blocking calls) in a closed loop.

We also provide access to data scientists who can adapt and refine the algorithms, or make sense of the patterns being detected, so fraud or IT teams stay one step removed from the technicalities. In due course, we'll also put more of this power into operators' hands through an 'analytics workbench' approach. The idea is that operator fraud teams will be able to control more of this themselves, without having to get down to the technical detail.

How soon will AI and machine learning become the de facto way to manage and guard against fraud for operators?

That's the million-dollar question. Really there is no time to lose. For now, it's the only way to comprehensively mine the enormous quantities of data, to find and shut down issues at speed and get ahead of the criminals. And in fact many operators are already using this kind of technology in other areas of the business – for instance as customer care interfaces (eg, chatbots), and in NFV automation. There is no question it should be applied to fraud monitoring as well – as it is in banking. There's no question that this is the way fraud management is going. And it pays for itself very quickly, in the losses saved.

What other systems and data could AI-driven analytics be applied to for fraud control, beyond those already being scrutinised?

AI can be applied to unlimited sources of data - structured or unstructured. So additional sources could include content data, social media sentiment, deep packet inspection data – there are really no limits.

> "Neural networks are ideal for the early detection of unseen threats in the area of fraud and security"

Usually we hear about big data analytics and AI being handled in the cloud, due to the superior scalability and economics when there are such vast data loads involved. Is cloud central to your solution?

Absolutely, but although our entire solution is cloud ready, most telcos are not. Telecoms operators are bound by greater regulatory control than their counterparts in other industries and so tend to be very nervous about letting sensitive data stray too far from their premises, even with the protection of robust data anonymisation. So we offer a range of options, including on-site and private cloud provision. Of course over-the-top digital service providers – the likes of Google, Amazon etc – use the cloud by default to manage sensitive data, so it's only a matter of time before telcos adjust, but for now we can support operators using whatever data handling measures they prefer.

What sets Mobileum apart from the competition?

We offer a very comprehensive solution, with several unique strengths. First, there's our telecoms industry expertise, and the deep knowledge and skills of our data scientists. Second, there's our unrivalled Active Intelligence platform. This combines a big data and AI capability with a service delivery and test platform, which can take action in the network based on any discovered insight, closing the loop automatically – for superior speed and cost-efficiency.

Lastly we can gain real market traction using our deep relationships with our many customers. We're significantly ahead in applying AI and machine learning to operator problems compared to our competitors, particularly in roaming, security and fraud prevention. We've been working with customers on these kinds of solutions for the last two years, so we already have a strong track record.

Is AI the be-all-and-end-all, or a complementary solution to existing investments?

It depends on the application. Our use of machine learning in fraud is much more effective for detecting and protecting against the unknowns, for instance, while known frauds can be still be effectively addressed with simpler rules-based systems. In the future, especially as more 'things' are connected over networks, smarter, learning-based techniques will absolutely be needed. Our solutions discover the fraud other systems can't – and at high speed. Already, today, this technology is saving operators from millions of euros of losses they would otherwise be incurring. Without doubt, AI-based analytics is the next essential investment in fraud control: the business case is robust.

About Mobileum

Mobileum helps CSPs leverage the power of predictive analytics to deliver monetisable insights that drive business transformation at 600+ CSPs across 150 countries. The company is based in California's Silicon Valley, with offices across the globe.
www.mobileum.com

The C-Suite

Interviews with senior execs from Europe's top operators

Tele2 Group CEO: From value for money connectivity to being an IoT titan

Tele2 is a past master among challenger brands, with reputation for market-challenging ideas, as well as commercial propositions. President and CEO Allison Kirkby talks to James Blackman about running a tight ship and having a right to win in the IoT space

Allison Kirkby, President and CEO at Tele2 Group, reflects momentarily on the unrelenting commoditisation of digital communications. "People don't want to live a life without connectivity and access to data," she says. "But this connectivity is often taken for granted – like electricity and water – and consumers don't want to pay much for it."

This is the lot of all service providers today – to develop incremental revenues from new and improved services in order to multiply out shrinking margins on old ones – and it is a game Stockholm-based Tele2 was born to play. Since its foundation in 1993, the operator has defined itself as a challenger to the former government monopolies and other established providers. Its corporate mantra, to "fearlessly liberate people to live a more connected life", reflects its drive to democratise telecoms services by matching them on performance and beating them on price.

"We are focused on providing [the] value connectivity our customers need, but at a great price," says Kirkby. It is the same code for every challenger brand in the market. The difference is Tele2 is an absolute master, sitting on the shoulder of the leading players in most of the markets in which it operates. Its latest results, for the first nine months of 2017, show its methodology is working. The group has seen mobile service revenues climb nine percent and EBITDA jump 25 percent. It raised its earlier profit guidance for the year as a result, to as much as SEK6.6 billion, offsetting a projected fall in sales and expenditure from the €95 million sale of its Austrian business to Three in August.

The flipside of this M&A activity is that it has bulked up at home, with the €300 million purchase of TDC's enterprise-focused Swedish division in late 2016. The company has been quick to merge the two operations, and strip out costs. "The complementary profiles of the two companies enable us to provide customers with greater value going forward. It is the perfect match, and we are already starting to see strong results and synergies from the integration," Kirkby says.

Tele2's commitment to delivering value means the group's running costs are tight, as a rule. "Being a challenger, it's critical we sustain a competitive advantage in our cost structure, so that we can continue to offer great value for money connectivity," says the CEO.

She notes that the company has started to "reap scale and efficiency benefits" more widely in 2017. Most impressively, it shrugged off a quarterly sales decline of six percent in the Netherlands to post EBITDA of SEK101 million, up from a loss a year ago. "The Dutch performance has undoubtedly stood out," the CEO says.

The company's various opcos have distinct roles and profiles within the group's strategy. Its subsidiaries around the Baltic Sea – at home in Sweden, and in Latvia, Estonia and Lithuania – are all well-established challenger brands, enjoying positions of some strength and generating considerable cash revenues.

By contrast, Kazakhstan and Croatia, as well as the Netherlands, are investment markets for the company, growing rapidly and approaching breakeven in terms of cash flow. Its joint venture in Kazakhstan, Altel, has seen two networks combine as one, and gain considerable efficiencies. "It is now a material contributor to group EBITDA," says Kirkby.

Its other going concern, in Germany, is engineered purely for cash generation. "We recognise we do not have the right to win in the long term, but we have a highly loyal customer base that we will take care of, and use the proceeds generated to invest back into businesses where we do have a right to win," Kirkby says.

New commercial focus

The group's growth has come from its new commercial focus. Kirkby's team has been restless in its marketing and propositions, seeking to encourage usage of its services and breathe life into its brand. In April, the company launched its "Power 2" marketing concept in Sweden with a series of new offers, including roam-like-at-home and unlimited data, which loosen traditional usage constraints and empower customers to make more of their communications.

They were attended by a new brand campaign, presenting Tele2 as the proprietor of a "School of Power", where pupils of all ages, and of every wacky demeanor, gain knowledge and inspiration to "use their digital powers fully". In May, in the Netherlands, it launched a "scandalously fast" no-limits data offer for €25 per month. The attendant advertising campaign retained the same bubblegum vibe as the School of Power execution. Most of Tele2's opcos have followed suit with their own roaming and data offers, as well as their own marketing treatments.

More generally, the boldness of Tele2's offers, and the energy of its marketing, is derived from its developing confidence in its own infrastructure. After heavy investment, its 4G networks in Sweden and the Netherlands, in particular, are firing. The number of 2G

Allison Kirkby, President and CEO at Tele2 Group

and 4G masts and base stations has increased by 140 percent in the north of Sweden and 40 percent in southern parts, for example. Tele2 made the biggest improvement for voice and data performance of all four Swedish operators in the latest benchmarking report from analytics firm P3, even if it trailed Telia overall. P3 noted the "huge efforts" Tele2 had made to improve its network during the past 12 months. Kirkby reflects: "The result is clear proof that our investments contribute to a more digitalised Sweden. But we are not yet satisfied and will continue to invest in existing and future networks."

Following several years of investment in the Netherlands, where the company offers only 4G services, Tele2 is starting to win business based on its network performance, she says. "We now have a network that is on par with the competition, and disruptive propositions that are better than the competition."

In the background, the group continues with its cloud strategy to have the majority of data and voice traffic on virtualised infrastructure by the end of 2020. Moving traffic to the cloud is a key staging post on the road to 5G, observes Kirkby. Tele2 has started the process in Croatia already, and will follow the same course at its other operations during 2018.

In parallel, it has signed a deal with Telenor, in Sweden, to extend its 4G network collaboration to build 5G technologies on shared infrastructure. "We are preparing for 5G, with higher speeds, shorter response times, greater reliability and more dense connection capacity. But the technology is not yet here and the use cases that will justify the significant investments ahead are unclear," says Kirkby. "Hence, our strategy is to be as prepared as possible to be able to quickly build and roll-out when the technology and use cases are available."

A titan of the IoT space

In the meantime, quite separately of its everyday operations, Tele2 has become something of a poster child among network operators in the burgeoning IoT market, a challenger brand that has assumed a position of leadership in the industry's most dynamic sector. The company is taking a horizontal approach, which sees it resell connectivity to a range of partners working in many different sectors.

"[The] IoT is somewhere where we feel we have a right to win, and so we are also investing into this small but fast-growing opportunity," says Kirkby. Tele2 IoT, established as a stand-alone business in 2014, has around 700 IoT agreements in place, and devices in 165 countries. It has just launched a new cloud-based routing solution, called 2ROUTE, which makes it possible to collect, route and manage IP data, from multiple cellular service providers in a single interface. Kirkby says: "We will continue to strengthen our horizontal offerings with exciting new products and services that will simplify and unify our customers' IoT solutions. Tele2 IoT is on a journey to become a titan in the IoT space."

Despite its slight detachment from the Tele2 family of businesses, its IoT unit fits clearly into its broader vision to lead the market for performance and beat it on price. "We have some of the world's best networks and we are single-mindedly focused on great connectivity aiming to enable as many as possible to benefit from that – whether they are individuals, households, businesses or machines," explains Kirkby.

"We know what it takes to build excellent networks, in a high quality but cost-efficient manner. By consistently passing on efficiency gains, we are stimulating connectivity and data usage."

TCTS: The new security paradigm for the networked society

There is a correlation between socioeconomic growth and trust, reflects Chalapathi Rao, Senior Vice President and CTO at Tata Communications Transformation Services (TCTS). "The development of society as a whole depends on its members' trust in its institutions. Technologies only gain acceptance when they are trusted by their users," he says.

But the industry has dropped the ball since the arrival of LTE-based technologies, he says, and stands to pay with its reputation and future growth. "This idea of trust has been seriously challenged by the move to 4G." Recent attacks on communications service providers, notably Deutsche Telekom and TalkTalk, are shots across the bow.

On one hand, the ecosystem has become intensely complex, and difficult to police. "This decoupling of hardware and software, this separation of compute and storage, presents a great dilemma for network security," Rao says. "The threat landscape has shifted with the technology, and no one knows where it ends."

As it turns out, there is a dark side to the industry's long-held dream of a networked society, being realised at last with the rise of advanced LTE-based technologies.

"Suddenly our identities are everywhere – as data in mobile devices, in vehicles, in smart buildings. That exposes us to risk – it threatens our finances, our personal data, even our safety. For this technology to be accepted and used, we have to be comfortable our identities will not be compromised," Rao says.

The CTO describes four major risks from unsecured networks: revenue, regulatory, reputational, and privacy. The industry is playing with fire. Even if the attack surface has been extended, the system's original architects have left backdoors open – everywhere.

Security is now high on the agenda. One such cross stakeholders collaboration project Rao points to is the 5G Ensure standardisation effort in Europe, which is focused on securing the next generation of heterogeneous networks, devices and services. Indeed, 5G makes the challenge more urgent, and the risks more alarming. Incoming LTE-based technologies signpost a giant leap forward for high bandwidth and low latency applications, including heightened concepts such as autonomous vehicles and remote surgery, which put human safety at stake, quite apart from privacy and security.

> "As far as possible, operators must ensure the digital security of every device on their network"

Two growth pillars

So what can be done to establish the kind of security that inspires confidence in the technology and growth in the ecosystem? TCTS describes "two pillars" for growth: digital identity and security automation. "If you're on journey of digital transformation, whether you're starting out or finishing up, then you need to understand these two pillars of digital security and security automation," explains Rao.

First, though, operators have got to get a handle on their own estates. "Everyone wants solutions, but first you have to check for existing vulnerabilities." TCTS claims to see "hundreds and hundreds" of vulnerabilities in operators' network systems. "Even if you put in 100 security solutions, it wouldn't make a difference because the networks have all these vulnerabilities already," explains Rao.

He makes reference to the attack on Deutsche Telekom last year, which impacted 900,000 subscribers, around five percent of its base, after a hacker attempted to hijack their routers. "It was an oversight – a silly mistake," says Rao, of Deutsche Telekom's failure to shut him out. "He didn't succeed, but there was an outage, and Deutsche Telekom had to offer compensation. It was a bad reputational loss." Operators have to focus on building in-house device security testing or vendor-independent teams to test such devices before commercial launch. Unbiased security reviews will avoid such incidents, which will occur frequently in future due to the exponential growth of IoT end points. TCTS, Rao points out, offers consultancy and managed security services. "Most security companies focus on IT, and not telecoms," he says. Network operators must get to grips with their own systems, and the vulnerabilities in them, before they contemplate tackling the end-to-end landscape.

"They have to assess and review the effectiveness and efficiency of their own security solutions. This is important. It has to be thorough," he explains. Hackers like low-hanging fruit, which is missed in most security sweeps. "Just one percent of attacks on network systems take advantage of discreet vulnerabilities; the other 99 percent simply trawl networked systems for easy openings."

The auditing of network security mechanisms and processes is timely as well. The General Data Protection Regulation (GDPR), to be introduced in Europe next May, will impact any organisation, anywhere, which handles data belonging to European citizens. The concept of ownership, and of personal data, is more

expansive, as well. "Penalties will be issued for any privacy breaches," notes Rao. "The industry has been warned; there are no excuses."

Digital identity

The number of connected devices is multiplying, and will rise ever higher with 5G after 2020. As far as possible, operators must ensure the digital security of every device on their network. To achieve that, devices must each have a distinct digital identity, in the first instance, to be traceable in the network.

"Their identity is very important; they have to be authenticated to be able to access the network, and to establish trust in the system," Rao says.

Identity is everything. Public key infrastructure must be the start-point in a robust security strategy; it is standards-based, well established and proven, and integrates easily with network systems. With strong digital identity, devices can authenticate when they come online and ensure secure and encrypted communications.

TCTS is pushing digital certificates as a trust model, to ensure every device and actor in the system is identifiable. From this, operators can establish robust identity and access management to enable the right individuals to access the right resources, at the right times and for the right reasons, ensuring compliance internally.

Rao makes the point that different systems require different security levels, and different compliance, and trust models based on identity and authentication can be managed accordingly.

In the new paradigm, security must also respond to changes in the system in real time. "You can't manage your network security manually, or with semi-automation. It has to be fully automated," he says. For security automation, the most urgent requirement is 'threat lifecycle automation' to address more threats, more quickly, with fewer resources.

"You can't wait weeks and months anymore to see where in the system attacks have occurred because the attackers are changing their identities like anything. So the threat lifecycle should be automated, external intelligence should be automated, alerts should be automated, testing should be automated, detection should be automated."

Chalapathi Rao, Senior Vice President and CTO at Tata Communications Transformation Services

Big data analytics, tailored for telecoms, underpins these automated processes. Rao points to the example of real time vulnerability management, allowing operators to absorb external cyber-security insights "on the fly" to rapidly detect and isolate vulnerable machines in the network. "This is very much required to tackle indiscriminate threats like ransomware, which targets multiple machines and companies," he says.

AI goes hand in hand, and will play an increasing role, he observes. "Another thing we see happening is the power of those things to predict these attacks, and then be able to automatically spin up new hardware and re-route traffic."

The risk is clear, and the question is plain. "If you put these devices onto your network without securing them, then they become your botnet – they are all open devices, which can be hacked," explains Rao. At the same time, for the wider industry, the choice is not a straightforward one.

Money gets in the way, naturally. The relative cost of securing a $400 handset is quite different to the cost of securing a $10 sensor, he observes. "What justification is there for putting very high security in very cheap devices?" Time-to-market is another stumbling block.

Worse, the industry only really contemplates security through the prism of its regulatory responsibilities, says Rao. "There is no in-built fear. Even the industry bodies, like the 3GPP, only think about security as much as they have to because security costs money, and they're influenced by the vendors. Vendors have so many boxes out there; replacing them all is inconceivable. Patching is the only solution."

In the end, TCTS says network operators have to take charge of their systems and processes, and develop clear strategies to secure them, which put in place identity and authentication tools, and automate security mechanisms as a matter of priority. Beyond this, it might just take the kind of large-scale breach that does irreparable damage for network security to be correctly perceived as priceless.

"Operators' brands are in danger. If they don't get it right now, one single attack could damage them beyond repair. That is not an exaggeration. The cost of a security breach in this new connectivity paradigm is huge, and causing jitters among operators themselves. They need to be very cautious and very deliberate in how they tackle their security challenge."

www.tatacommunications-ts.com

Is Your Network Burdened by Excessive Signaling Traffic?

NetNumber dramatically simplifies your signaling infrastructure, enabling you to innovate new services in:

- IoT and M2M
- Private LTE Networks
- Signaling Security and Robocalling Protection
- Mobile Edge Computing
- 5G
- NFV and SDN

Learn why hundreds of CSPs trust us @ www.netnumber.com

NetNumber

Special report
SECURITY

24

26

Contents

Sponsored By

NetNumber

Q4 survey: Industry is confident despite rising cyber threats, lack of skills

The telecoms industry thinks it is doing a decent job overall when it comes to protecting retail customers, but is conscious there are improvements to be made. Marc Smith reports

How good do telco execs think the industry's reputation for security is with retail consumers? Pretty good, it turns out. Respondents to European Communications' latest quarterly survey return a weighted average of 3.2 out of 5 to this question. Telcos are "probably the most trusted partner there is," according to one respondent, although another warns that "best practice is well understood, but not always funded". At the other end of the scale, one respondent notes: "Reputation is bad because of recurring incidents with third parties breaching private data held by service providers".

True to form, operator respondents give themselves a slightly higher mark, 3.4, than the rest of the industry. But the majority of operators who took the survey, 60 percent, say cyber attacks on their companies have increased this year. In spite of this, 77 percent say they are either very or relatively confident that they can keep their customers safe.

The wider industry is not so sure. Over half of all respondents, 53 percent, think operators are not doing enough to protect their customers. "They can, and must, do more," according to one.

Meanwhile, the survey reveals that the biggest challenge to the success of operators' security strategies is cultural not technological. Just shy of two-thirds of all respondents, 64 percent, say improving culture is a bigger hurdle for operators to overcome than improving technology. "Technology can be more effective with [better] culture and user behaviours," one writes.

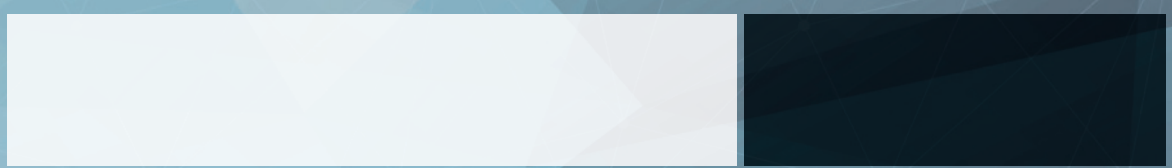
Operators seem to be aware of this. The majority of them, 51 percent, say they did not have enough of the skills they needed to currently deal with the security situation. They also appear to be acting to cover gaps. Another majority, 54 percent, reveal investment dedicated to security in the current financial year has increased.

Mobile-related products and services are viewed as posing the biggest security risk to retail customers currently, while organised crime comes top of a list of actors posing the biggest threat to operators themselves.

Looking ahead, the industry remains upbeat. Sixty one percent of respondents think it is possible for operators to stay ahead of the curve when it comes to security threats. One notes the comparative lack of data leaks at telcos compared to OTT players. But another warns: "In my experience, operators tend to operate with general paranoia rather than properly thought through threat models; could do much better!"

The full results of the online survey, which polled 168 people between October and November 2017, can be viewed over the next few pages. Forty two percent of respondents work for network operators, 25 percent for vendors, while the remaining 33 percent include analysts, consultants, trade bodies and governments. Seventy one percent of respondents are based in Europe.

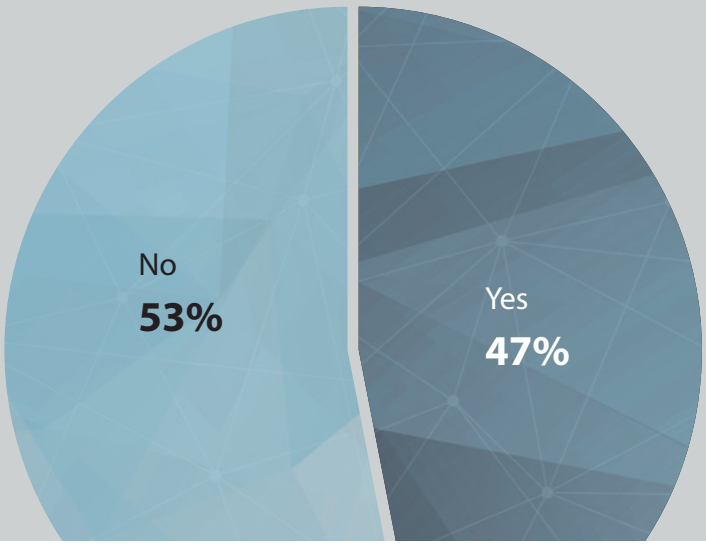
How good do you think the telecoms industry's reputation for security is with retail consumers?



0 (Very bad) **3.17** **5 (Very good)**

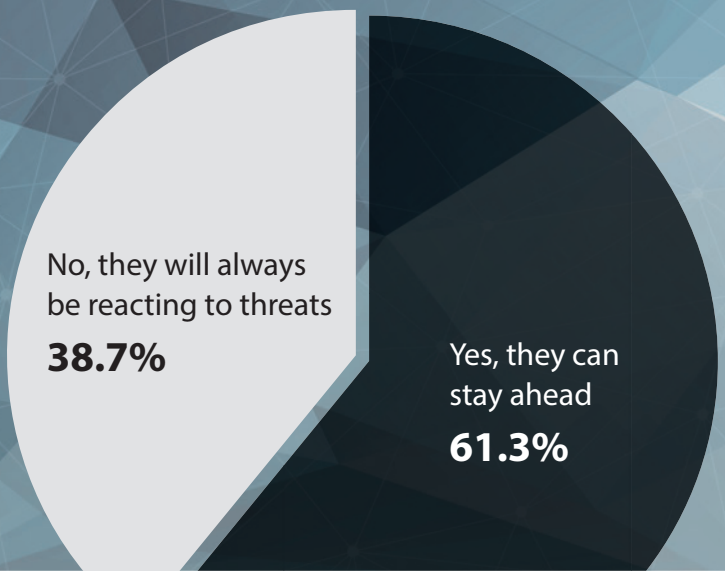
*All respondents

Are operators doing enough to protect their retail customers?



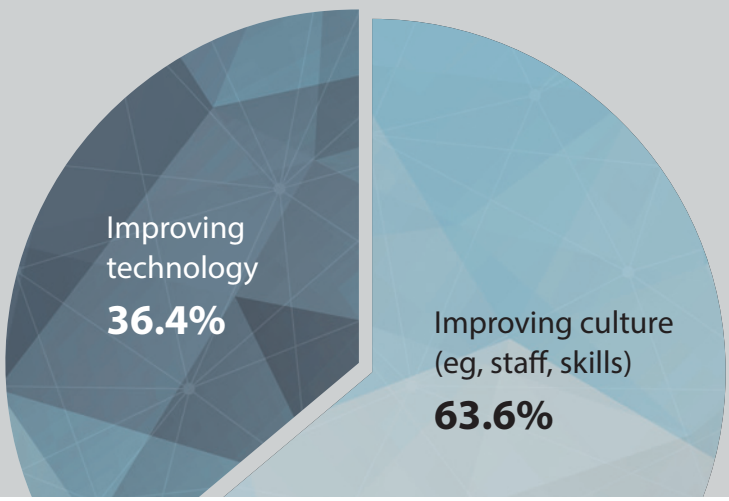
*All respondents

Do you think it is possible for operators to stay ahead of the curve or will they always be playing catch-up to security threats?



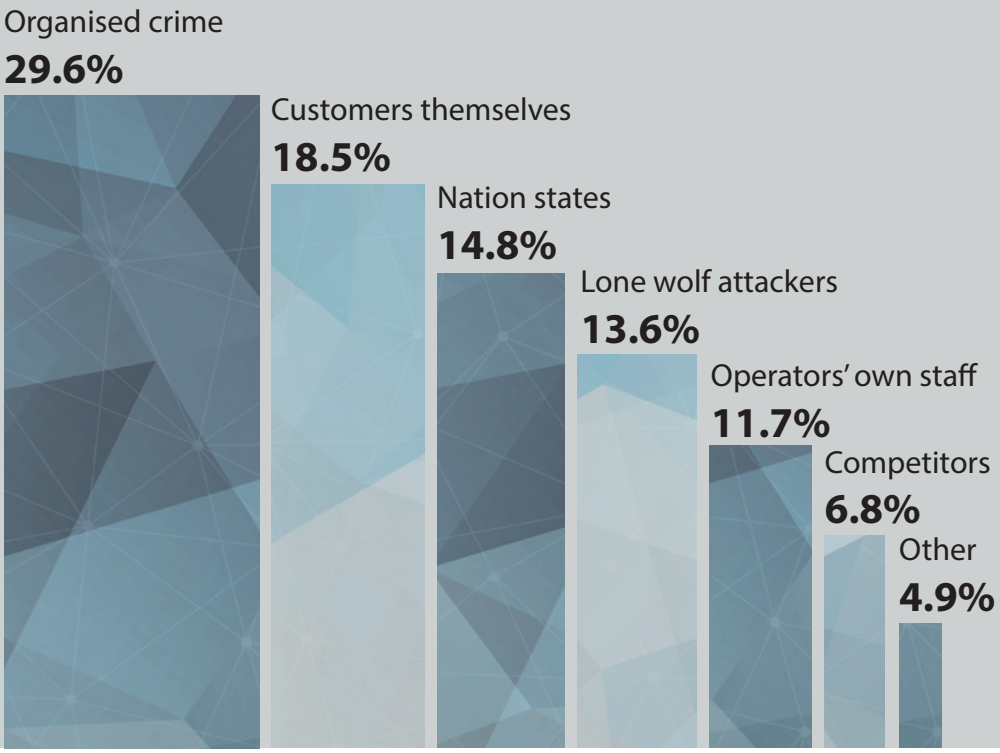
*All respondents

Which do you think is a bigger challenge to operators' security strategies?



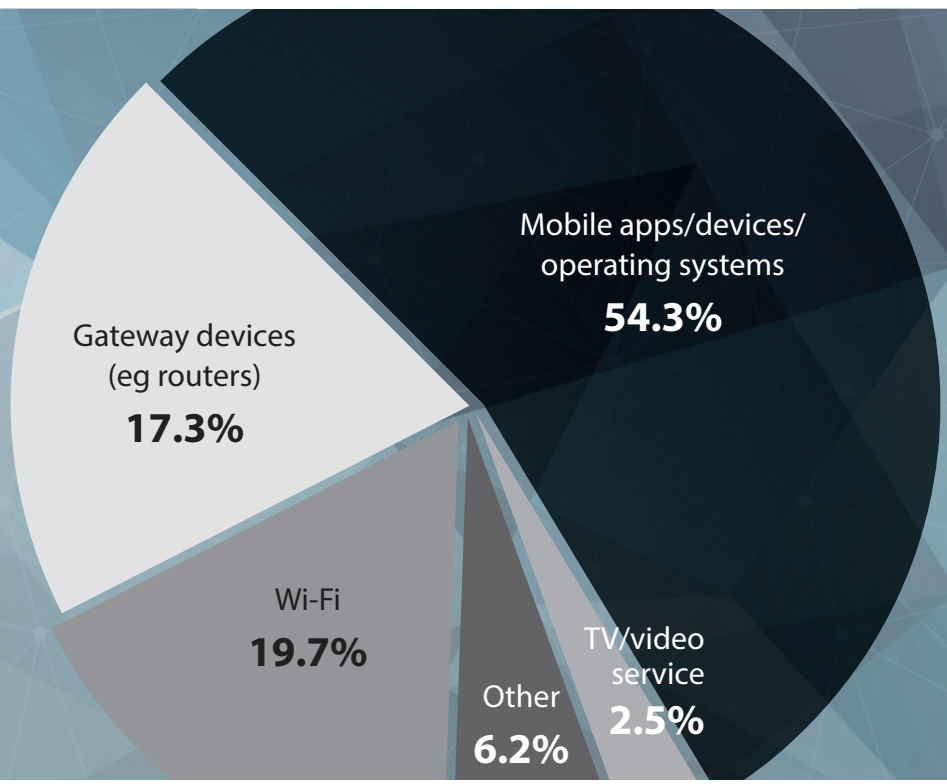
*All respondents

Which actors do you think pose the biggest threat to operator security?



*All respondents

Which third-party technology do you think poses the biggest security risk to operator's retail customers?



*All respondents

How many staff do you have dedicated to security currently?

0-10
20%

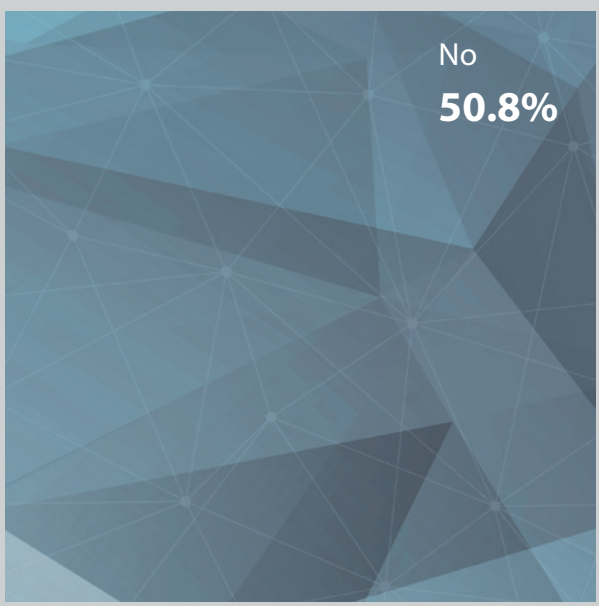
11-50
40%

51-100
10.8%

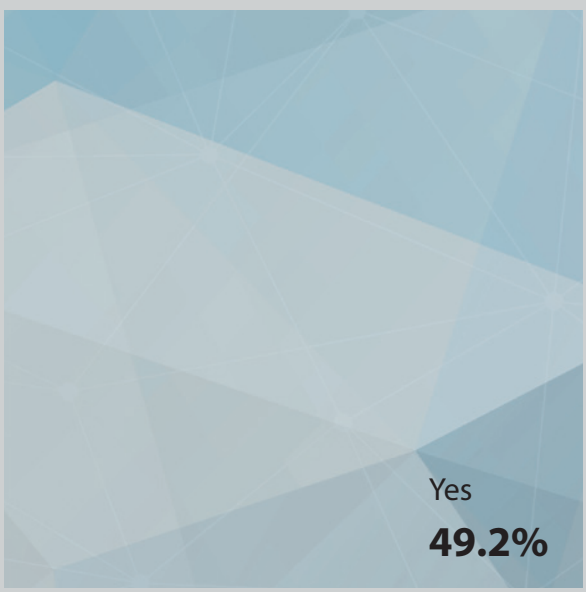
More than 100
29.2%

*Operator respondents

Do you feel you have enough of the skills you need to deal with the security situation currently?



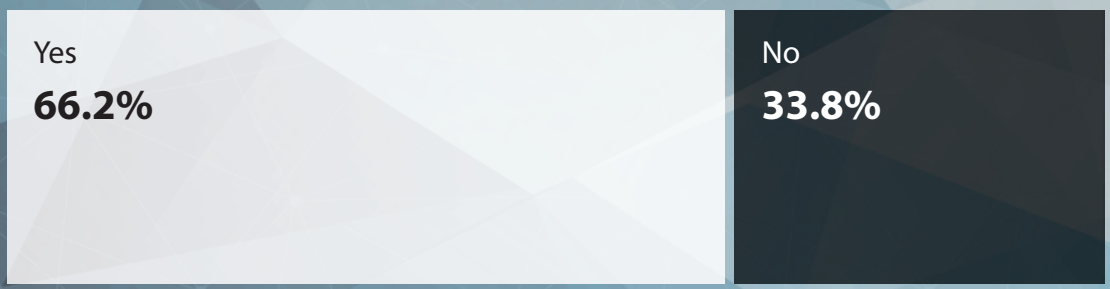
No
50.8%



Yes
49.2%

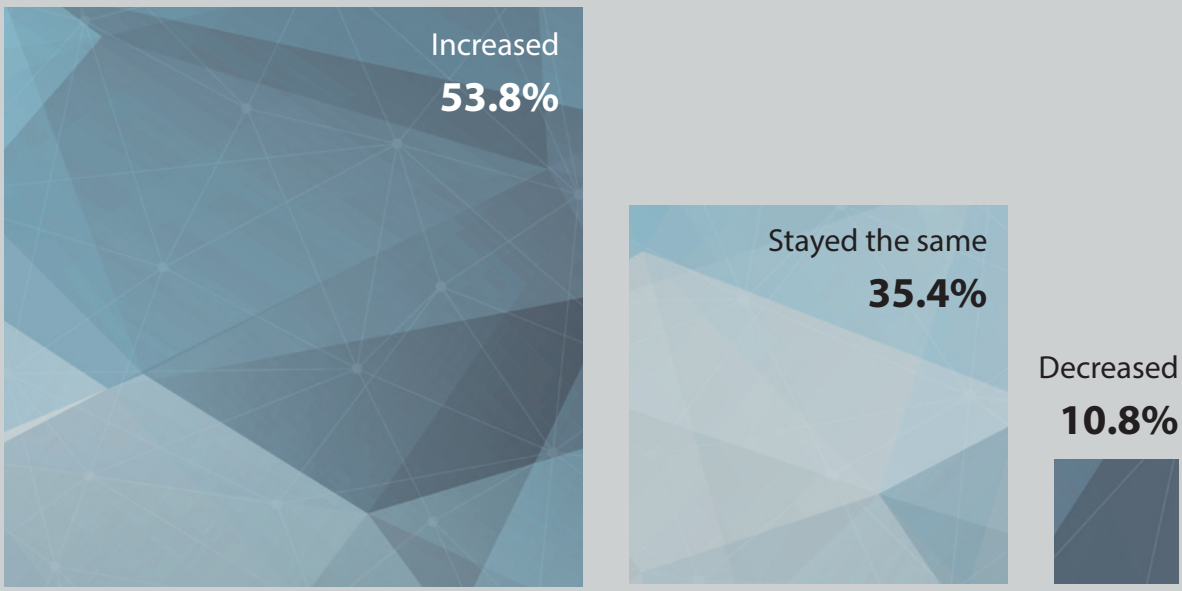
*Operator respondents

Do you think your company is investing enough to protect its retail customers currently?



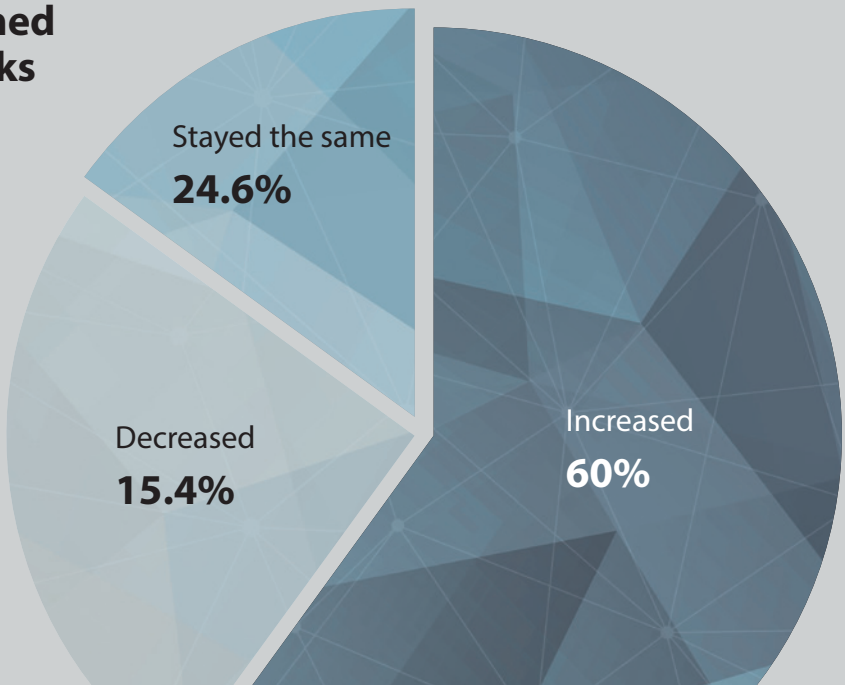
*Operator respondents

What's happened to this investment dedicated to security in the current financial year (versus the previous year)?



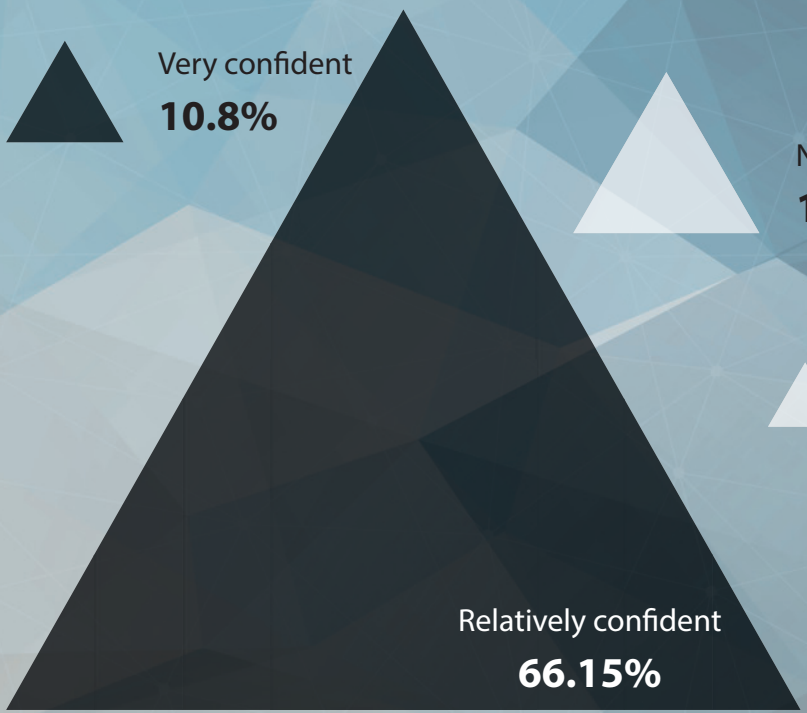
*Operator respondents

In 2017, what's happened to the number of attacks on your company?



*Operator respondents

How confident are you that you can keep your company and your retail customers safe?



*Operator respondents

One year on: Deutsche Telekom's lessons from front line of cyber security wars

Dr Rüdiger Peusquens tells Marc Smith how the German operator plans to protect its customers following an incident that saw 900,000 routers taken offline last November

Deutsche Telekom's Vice President of Cyber Defence Response was on his way back home from a weekend trip in November last year when he got the call that all was not well. Although Dr Rüdiger Peusquens didn't know it at the time, the Germany-based operator was the unintended victim of a malware attack created by a gun-for-hire called Spider-Man.

The hacker, who court documents show wanted to pay for his upcoming marriage, had been hired by an unnamed telco in Liberia to knock out a local rival but ended up causing 900,000 Deutsche Telekom routers in Germany to go into meltdown. Customers were unable to use the company's services for up to several days as the routers overloaded and crashed.

Deutsche Telekom followed journalist Brian Krebs' website, web hosting provider OVH, Oracle-owned Dyn and Irish operator eir in being on the receiving end of a Mirai-based hacking attempt. The smoking gun for these was the publication of the Mirai source code on the internet in August 2016. This gave any hacker the opportunity to develop their own bespoke version of the malware and create an army of botnets to attack a given target.

Spider-Man chose routers as the vehicle for his intended attack and, by chance, ended up targeting a batch belonging to Deutsche Telekom. ABI Research Analyst Michaela Menting suspects the hacker used a website called Shodan – "Google for IoT devices" as she puts it – to find devices that were not protected by authentification mechanisms that would deny access to unauthorised users. Unfortunately for the German telco, its routers fitted the bill.

Dr Rüdiger Peusquens, Deutsche Telekom's Vice President of Cyber Defence Response

Peusquens' team became aware that something untoward was happening when "changes in network traffic" were noted. When consumers started having problems – Peusquens calls this "collateral damage" – it was clear a serious incident was occurring.

The silver lining to this particular cloud was that Spider-Man was too ambitious. The malware was supposed to infiltrate the routers and sit dormant until the attack was ordered. However, an extra instruction he had added to his version of the Mirai code – to eliminate competing strains of the malware – was too much for the routers to handle and caused them to crash. Software updates were sent out within 12 hours, Deutsche Telekom's own network was unaffected and life started to get back to normal.

Security by design

Twelve months on from the incident, and with Spider-Man now in jail, Peusquens is keen to set the record straight. "We had two router [types] that went down under the sheer load of traffic," he says. But he adds: "To be clear this was not because the attack was successful." Peusquens is very keen to point out that a lot reporting of the event at the time – that Deutsche Telekom was hacked – was incorrect. In short, he says it was an attempted hack that failed but had consequences for the operator's cus-

tomers. "This was not an attack against Deutsche Telekom," he reiterates. "It was a worldwide attack to take over DSL routers." If some journalists have to raise their hands up to having made a reporting error, what about the German incumbent? "I don't think we could have done anything differently to prevent it," responds Peusquens. "There's always something you cannot test. Our processes worked well. We didn't have to fix anything as such."

While the operator's customers may choose to disagree, Menting has some sympathy with this view. "What should be done with a lot of IoT devices is to implement security at the design phase," she says. Citing the likes of dynamic passwords, she adds: "In their risk assessments router manufacturers don't take into account that other malicious actors seek to use them for their own purposes. The mindset is to think that it only happens to PCs and smartphones, not dumb routers. Why spend the money when it's not going to happen anyway? That's the mentality of a lot in the industry who don't know a lot about security."

Peusquens points out that routers, and much more kit besides, must adhere to Deutsche Telekom's own security requirements. "We do our own hacking tests," he explains. "If we find anything we send it back to the manufacturer to be fixed."

But he notes: "Some manufacturers do not provide an update if there is a security flaw and this enables huge botnets." As Deutsche Telekom found out, more often than not criminals are ahead of them. But Menting thinks telcos should and could be doing more. "Telcos need to educate consumers that their routers can be vulnerable but that they can change their passwords," she says. "By not informing users it's down to the telco to accept the risks."

Peusquens maintains that the operator's reaction was "quick" and the feedback it received was largely "positive". Stats bear out this upbeat assessment – the company added 270,000 broadband lines between the end of September 2016 and the end of September this year.

Big business

Whatever the rights and wrongs of the episode, it seems everyone will have to get used to more of these incidents in future. Peusquens describes DDoS attacks as "big business these days" and a threat that is "growing dramatically". Deutsche Telekom "frequently" sees hacking attempts on its network, he says. While the attackers haven't been successful "so far", he admits "staying ahead [of them] is difficult because attackers are always coming up with new ideas".

The operator has even received blackmail threats that promise an attack if a ransom paid in Bitcoin is not received, according to Peusquens. More worrying, he notes, are the groups that "silently look to infiltrate networks be it for political reasons or espionage. This is very dangerous because it's hard to detect," he says.

What about the fact it was another telco that instigated the November 2016 attack? "Of course it's not the way we want to work with our competitors," says Peusquens with a degree of understatement. "But even in telecoms there are black sheep. What I like is that the guy who did it was caught and sentenced – laws apply to cyber space as well."

The biggest challenge, according to Pesquens, is ensuring you have "the right alarms". He explains: "If you catch a burglar breaking into your house, it's better than catching him after he's opened your safe. It's the same in the cyber world."

Crucially, Peusquens says it is important to accept that you cannot protect all of your assets all of the time. "It's not efficient and it costs a lot of money," he explains. "We have to accept we're under attack… the challenge is to catch [attackers] early on. It's like a fire – we don't have open fires in the house, but we do have smoke alarms and the fire brigade around the corner. In the cyber world, we don't switch off firewalls and anti-virus but we have to be aware that they do not protect you entirely."

ABI's Menting agrees that the cost of making every internet-connected device as secure as it can be is "significant". Nevertheless, she says there needs to be a sea change in attitudes. "We need to stop viewing security as a cost but as a necessary element, as intrinsic to the functioning of internet services that we take for granted," she says. The analyst likens the current situation to one played out by the automotive industry in the past. She says car manufacturers initially battled governments over the cost of adding seatbelts and airbags to vehicles. Buying a car without such safety features is now not only unthinkable, but also illegal.

While regulation to make routers and other devices more secure is some way off, Deutsche Telekom is working hard to mitigate the risks. The company's Cyber Defence Centre aims to identify patterns of behaviour that point to cyber attacks, for example. The centre, which employs some 200 people "around the clock", claims to analyse around one billion pieces of security-sensitive data every day from some 3,000 sources. It even has its own "honeypots" to bait hackers and thereby expose the techniques they are using. As well as protecting the operator's own systems, the centre also protects over 30 companies in Germany. It is a key part of Deutsche Telekom's new Security business unit, which launched in January this year to oversee all of its work in this area. Peusquens remains "very confident" about Deutsche Telekom's ability to handle the ever growing threat landscape. "We can fight them," he says.

But Menting warns that the November 2016 incident should serve as a wake-up call if telcos are serious about moving into new areas. "They are not just going to be providing internet services in the home, they're also going to provide them in cars, in planes so [attacks like] Mirai could have a physical impact. If a hospital is offline then that's a completely different level."

Cyber security brings dynamic new revenue opportunity, execution challenges

Operators might have found a killer app at last: the provision of cyber security services to businesses. James Blackman reports on the opportunities and obstacles that exist and what the industry needs to do to turn this vision into a reality

Cyber security presents a multibillion-euro opportunity for network operators with the tools to help enterprises protect their business information and intellectual property. With each high profile cyber attack, interest in their security solutions jumps, and their revenues get a much-needed boost.

In general, non-core services such as cyber security contribute only about five percent of telco revenues, according to Gartner. The figure rises as high as 15 percent among the most digitally progressive, however.

Security tops the charts for tier-one providers, ahead of cloud services and IoT technologies, scoring 60-70 percent growth in 2015/16 and 35-45 percent last year. "It's still very high, compared with other non-core services, and it will pick up again," remarks Gartner's Gyanee Dewnarain.

Recent incidents, notably the Wannacry virus in May, will likely show in the credit column next time out. "Enterprises are wondering what to do about security, and operators are seizing on that," adds Dewnarain.

The logic for operators, providing and protecting access anyway, is plain. "The danger of DNS attacks, in particular amplification attacks, is of particular concern," says Michela Menting, of ABI Research. They are already securing their networks with DNSSEC, IPsec and SSL/TLS protocols. That's just the start, she notes.

"Investment in back-end software and hardware components has been complimented by standards development, regulation, certification mechanisms, best practices, and guidelines for cyber security preparedness, as well as capacity building and organisational efforts."

The open nature of the internet is a boon for cyber criminals and the threat landscape has enlarged, way beyond its old boundaries. "The traditional security perimeter for enterprises has dissolved," says Les Anderson, VP of Cyber Security and Chief Security Officer at BT. "While technologies like cloud computing and mobile devices have the potential to make organisations more agile, efficient and competitive, they have also introduced a multiplicity of new security risks."

Operators, continuously tested and trained, are well positioned to re-sell their hard-won expertise. "Telco data is extremely valuable, and malicious third-parties want it. This has forced us to learn, prepare, and work faster than others," remarks Nikolaos Tsouroulas, Head of Product Management at ElevenPaths, Telefónica's cyber security unit. The Spain-based operator employs 1,000 security staff and 650 analysts in seven security operations centres (SOCs) around the globe. "It is natural customers want security from the same party that already supplies their communications," says Tsouroulas.

Unlike others, Telefónica is "not just a reseller" of security services, it says, but a developer of anti-hacking tools as well. ElevenPaths has registered 15 patents in four years, all for technologies it has developed in-house; many inform the industry's broader fight. The company also claims a strong publishing record, of proofs, investigations, and academic research. "Our strength is our people," remarks Tsouroulas.

BT, the only FTSE 100 company authorised to accredit its own systems and networks for UK government use, has 3,000 security professionals in 15 SOCs, variously scattered. "As both a network operator and internet service provider, we are trusted to help repel cyber threats on behalf of the UK. This gives us accurate up-to-the-minute information of any oncoming DDOS attacks, visibility of the origin of phishing attacks, and the oncoming threat of advanced persistent threats," says Anderson.

BT points to its use of artificial intelligence to keep customers safe. Its "machine-assisted cyber threat hunting technology" uses visual interfaces to identify and understand cyber security threats in huge large amounts of data. The company also claims to be the first to launch ethical hacking for corporate clients, to test systems and flaws, and rate overall effectiveness of their security set-ups.

Like Telefónica, Orange has made the case to hive off a dedicated security business. Its Orange Cyberdefense unit, a function of Orange Business Services, employs 1,200 experts in six SOCs. "Orange Cyberdefense relies on Orange's strength and its position as an operator," says Michel van den Berghe, its CEO.

Specifically, it hinges on three network assets: the ability to install probes to collect data and detect weak signals before an attack occurs; the ability to "clean the flux" where the attack is happening; and the ability to help customers compartmentalise the network to stop attacks from spreading. "Orange's role is to provide people with access to the Internet. It is also our role to secure this access," says van den Berghe.

As well as an epidemiology laboratory, and two DDoS 'scrubbing centres', Orange claims it is "the only operator to have its own CERT", or computer emergency response team, to deal with attacks. It is based in France, with representatives in Montreal and Singapore as well. Menting suggests that "many telcos" in fact propose CERT and SOC functions to their business clients, as well as running them for themselves.

Execution, collaboration and innovation

This trio is among the leaders for re-selling cyber-security defences to enterprises. Defined as managed security service providers (MSSPs), they are distinguished from a following pack that has until now only flirted with point solutions for network-related security.

"The managed services or security-as-a-service market is a popular offering, especially to businesses that want to run their own private networks over public networks. This includes managed PKI services, security certification schemes, the offer of anti-malware and anti-spying tools, and VPN services," comments ABI's Menting.

But the security offers of tier-one telcos are advancing rapidly. As attacks have succeeded, and interest from the market has grown, competition among them has increased. Where they have for some time offered neatly packaged bundles of cloud and on-premise security solutions, as MSSPs, they are now attempting to provide the whole lot, namely audit, design, protection and analysis. Their scope has moved beyond network security to cover the broader IT set-up.

"There was a transition, when the old MSSPs realised there was such huge growth in the market – when it started to get crowded and competitive, and their profits started to fall. Instead, they have started moving towards end-to-end solutions, covering all elements – including consultancy services, professional services, managed services, and intelligence and analytics," explains Gartner's Dewnarain. These four components go from initial risk assessment, through to the design and management of security systems, and ultimately to threat forecasting. It is where all the major operators, including BT, Orange and Telefónica, are now focused.

Of the four disciplines, the last is the most dynamic and powerful. "Threat intelligence offers the highest value in that end-to-end chain, and that comes down to analytics, big data and machine learning," says Dewnarain. "That is where the battle is – how to predict attacks before they happen. You need strong apparatus to do that, and operators haven't traditionally had them. If they take the right actions – if they partner with the right organisations, and make the right investments, as BT and Orange appear to be doing – then, yes, they will be competitive."

But review and recommendation, the first principles of a thorough security strategy, is of increasing importance, too. "One of the problems is enterprises often don't know where to start with cyber security, despite their concern with it," explains Dewnarain. "Operators need to get more into that business consulting play, which again isn't a core competency."

Where they don't have the capabilities, they are recruiting talent, making alliances, and buying expertise in. "They need to either partner with specialist companies or recruit well," she says. Orange Business Services has acquired French security companies Atheos and Lexsi in recent years. Telefónica has acquired Spanish firm SmartAccess, and taken a stake in Blueliv; it acquired Informatica 64, the previous incarnation of ElevenPaths, back in 2013.

Given the increased attack vectors, security consultancy services represent the most dynamic form of business development for network operators. "If they get that part right, then it opens the doors for the other elements of the value chain. If they don't, they'll lose the opportunity completely."

With the provision of cyber security services, the operator community, in neverending pursuit of new opportunities, might just have found its 'killer app', at last. They have hard-won credibility and great form; the field appears to wide open, as well – and notably void of OTT providers, which have provided their most decisive competition in the consumer content market.

"They have a competitive advantage, and they don't have competition from the OTTs this time," notes Dewnarain. "But they have been in this position many times before. The execution matters – as does collaboration and innovation. It is a great opportunity, and they get it. It is just down to them how they capture it. Some are doing really well, but the battle is not won. The question is whether they are going to be agile enough."

NetNumber: Operators must fight SS7 hackers with data insights

The mobile industry has been caught short as hackers have discovered an easy backdoor into essential network technology underpinning communications for 30 years. They have found they can snoop on private data and communications, and track users' movements and activities.

Specifically, they are gaining can access to the SS7 protocol stack, which allows networks to exchange subscriber information for mobile roaming services. Criminals have hacked data in the SS7 system to redirect calls to premium numbers, eavesdrop on calls, do location tracking, and even intercept two-way SMS authentication, often in combination with sophisticated phishing attacks, to gain access to private accounts. Earlier this year, hackers exploited the flaw to hack into mobile users' bank accounts in Germany.

In theory, they might even use the SS7 system to down network services altogether, as Telenor discovered in Norway in 2016, when an SS7 security company inadvertently hit upon a fault in its home location register (HLR), and knocked out coverage. Ultimately, the Telenor outage was accidental and quickly patched, but it made clear the system's vulnerability.

The impact is damaging at every level. "The operator's credibility is questioned, and individuals are targeted," explains Pieter Veenstra, Senior Manager of Product Development for Security and Routing at NetNumber. "Banks and other service providers are impacted as well." The IoT will mean signalling control becomes even more complex and vulnerable.

NetNumber has a solution that is the best defence available to operators against SS7 attacks. It comes as part of its core TITAN software platform, which enables operators to simplify, scale and secure their signalling control networks, which manage such functions as subscriber profiles, policy servers and access control servers.

Veenstra is the industry's most senior authority on signalling control; resident expert at KPN in the Netherlands for 30 years before joining NetNumber four years ago as a product manager for TITAN, from which all its signalling solutions spring. His exit from KPN was part of the wider exodus of engineering talent from operators. "Operators started outsourcing technology, and I am a technology nerd," he reflects.

> "Hackers have learned the weaknesses of the networks; they know how to bypass existing filters"

At NetNumber, he has focused on security aspects of signalling control for the last two years, and served as chairman of a working group within the GSMA's Fraud and Security Group on signalling firewalls. Signalling systems' security has become a hot topic, as inherent vulnerabilities in the fabric of telecoms infrastructure have been fiercely exposed by hackers, and revealed further in Veenstra's own research with the GSMA.

Lessons from history

It wasn't always like this. SS7 has been the default signalling protocol for packet-switched communications since at least the early 1990s. Such attacks were then practically unheard of – SS7 was effectively secure, accessible only by physical means. The flaw has only really been exposed and magnified since the rise of IP communications, and the ubiquity of smart devices fuelling mobile roaming services. "That's when the problems started to hit," says Veenstra.

The exchange of mobile roaming data has provided fertile hunting ground for hackers, making the issue suddenly a desperate one for operators. Indeed, despite its vintage and the emergence of new signalling protocols like Diameter and SIP, traffic through the SS7 control network is still rising as smartphone ownership and usage continues to spiral upwards. The introduction of 'roam-like-at-home' regulation within the European Union has also buoyed the SS7 data exchange.

At any time, an operator is exchanging roaming data with around 1,000 other providers, says Veenstra, from the planet's biggest brands to its most marginal. "This mobile roaming traffic is going end-to-end, which makes it tricky," he explains. The issue is operators cannot be sure their roaming traffic is from a trustworthy operator source. Providers are selling wholesale access to the SS7 signalling network "at a very reasonable price", potentially opening up the whole system to fraud.

"Mobile operators have been caught out; a few years ago, they started to implement signalling firewalls to protect their networks," says Veenstra. These firewalls will be required to filter massive volumes of events in the next years, as the IoT takes hold, interconnection scenarios multiply, and the attack surface is re-defined.

Filter tips

NetNumber is at the forefront of research and innovation in signalling control. In 2016, it took the initiative in the GSMA Fraud and Security Group to define industry requirements for SS7 sig-

nalling firewalls. The resulting document, GSMA standard FS.11 v3.0, published last November, contains most SS7 vulnerabilities and provides guidelines on firewall rules and managing risk.

Its own signalling firewall claims advantages in terms of redundancy, reliability and performance as part of the TITAN platform. The SS7 application provides multi-layer threat evaluation (MTP3, SCCP, TCAP, and MAP/CAMEL) and augments other SS7 applications available on TITAN including STP, HLR, EIR, and SCP. Importantly, it offers the same capabilities for other existing protocols, including Diameter and SIP, and HTTP/2 and JSON, which will arrive with 5G.

It stands out because of the depth of the analytics that inform its filtering mechanisms. Its Global Data Services analytics platform collects and processes data from around 1,000 interconnected communications providers and other agencies. "Firewalls are only as good as the data in the whitelists and blacklists of their filters, and filtering is only as good as the counter-intelligence behind it," says Veenstra.

"Hackers have learned the weaknesses of the networks; they know how to bypass existing filters. Operators have huge problems keeping the data of their filters up to date and complete. Our global data feeds make their filters very precise – the number of false positives is minimised, the protection is enhanced tremendously. The data we are using to whitelist and blacklist is really a different shade to what others can offer and it means staff are released from provisioning because we are feeding the filters to whitelist and blacklist traffic and events on the network."

Configurability is another distinguishing mark, he adds. New rules can be easily programmed to filter roaming traffic and protect the network. "This is particularly useful to protect the interconnects with national MNOs and MVNOs. It also enables the operator to enhance very easily the protection of its SS7 signalling firewall against new attack scenarios."

Its support for multiple signalling protocols is also notable, and fits with NetNumber's essential business proposition – to offer operators a way to manage a single software-based signalling platform from one supplier, instead of running three separate signalling control networks and 20 related functions from a roster of vendors.

"It is a future-proofed solution," says Veenstra of its multi-protocol firewall offer. "It doesn't make a difference to us whether location messages are sent in SS7, Diameter, SIP, or even HTTP/2 in the future – they are all treated the same way. Competitors are offering one or the other. We can handle all of them. We are prepared for the future. "

New challenges

As operators transition to Diameter or SIP based communications, the interworking of signalling control protocols complicates security and exposes further threats. For Diameter, NetNumber has been again coordinating the standardisation track in the GSMA working group, with around 55 security experts, compared with just 15 experts for the work on SS7 signalling firewall.

Half of these experts are from the operator community; a sign of the seriousness of the issue. "Operators are really concerned," says Veenstra. In August, his signalling group at the GSMA published FS.19 v2.0, containing Diameter firewall rules and data sharing guidelines. The heightened complexity of the security challenges with Diameter signalling is palpable.

"Diameter replicates the same security problems from SS7, because the same roaming procedures are being copied, so the same attacks will happen. But the problem is greater because the visibility of who is sending the requests is hidden due to network topology hiding," he says, explaining the inner-workings of international signalling. "In SS7, the answer message never returns to the attacker. In Diameter, the attacker gets the answer back."

It makes identity and authentication, the cornerstones of any security protocol, redundant. The challenge of security in Diameter signalling is compounded by its sheer complexity, with nesting of grouped AVPs, or value parameters, and different encoding schemes creating additional layers. The latest GSMA risk classifications for Diameter run to three Excel pages, ranging from 250 up to 1,000 entries, notes Veenstra; the same review of SS7 vulnerabilities is but a single page, albeit an extensive one.

A second GSMA release of Diameter firewall guidelines is likely at the beginning of 2018. But work is slow, he notes. "Since the problem is so complex, operators are already starting to ask if they will use Diameter for roaming services at all, and extend lifetime of SS7 instead, and then go straight into an HTTP type of solution. So it is that serious with Diameter."

For now, both attack and defence is focused on the SS7 signalling control system, and NetNumber's configurable, data-driven solution is turning heads. "For SS7, we are confident our signalling firewall gives the protection required by the GSMA, and goes further than that because of the flexibility to add more filtering rules for specific network situations."

It is picking up both business and awards, having bagged one for the most robust IMS security solution at the IMS World Conference in May, and one for best new security solution at the SDN NFV World Congress in October. Its clients are naturally sensitive about security, and do not wish to go public, but at least a couple of tier one global operator groups have signed up in recent months alongside a bulging roster of tier two and three brands.

"We are very fortunate they have selected our solution. Those mobile operators have strict requirements, which have tested us, and been very good for us," says Veenstra.

www.netnumber.com

NetNumber

CMO roundtable: Striving to lead the telco transformation

Past and present CMOs took part in European Communications' annual roundtable in October to discuss the state of telco marketing and the struggle to put the discipline at the heart of efforts to transform operators. Alex Sword reports

CMOs retain a somewhat ephemeral existence within the telecoms industry; a key part of the executive committee at some operators, non-existent at others. Yet marketing is, arguably, an increasingly important discipline if operators want to become so-called digital service providers. The range of responsibilities held by participants at this roundtable demonstrate the evolving nature of the CMO in 2017, and the road that is still to be travelled if marketers are to make their voices heard in the boardroom.

At Three UK, the CMO role was created a few years ago as part of a wider overhaul at the company. "Our perception years ago was we were cheap and rubbish", says a refreshingly honest Tom Malleschitz, who moved from being CMO of Three UK to take up a new role as Chief Digital Officer in December 2016. What he calls the strategy of "winning the battle with the cheapest price and the rubbish network" brought the company to a certain point, but Three needed scale. "The change [we made] was to place employee engagement as the number one KPI and net promoter score as the second most important," says Malleschitz. "The whole industry sucks but we were the worst, which wasn't good. But we said, ok, if we do these two things right, the EBIT growth will come automatically."

The results are encouraging – the company has seen its customer base double between August 2010 and June 2017 to 12 million. Malleschitz answers in the affirmative to European Communications Editor Marc Smith's question as to whether marketing is more important for a challenger than an incumbent telco but, due to financial pressures, thinks it is becoming ever more crucial for established operators.

Olivier Crucq, Director of Consumer Marketing & Strategy at Belgian incumbent Proximus, moved over from heading up the operator's enterprise division in January this year. He says it is an "interesting time for marketers" at the telco, almost four years after Dominique Leroy was appointed as CEO with the explicit objective of making Proximus a "marketing-led company". Unlike previous CEOs, Leroy comes from a marketing rather than financial background.

Crucq agrees with Malleschitz, saying this is a new direction for an incumbent telco, which traditionally are more driven by the network and engineering. Now, the strategy "starts with the consumer".

Participants

Ismail Butun,
CMO, Turkcell

Olivier Crucq,
Director of Consumer Marketing & Strategy, Proximus

Ranko Jelaca,
CMO and CCO, Telekom Slovenia

Anthony Kendall,
Strategy Director, Brand Finance

Tom Malleschitz,
Chief Digital Officer, Three UK

Kester Mann,
Principal Analyst, CCS Insight

Marc Smith,
Editor, European Communications

This has meant the creation of "marketing designers" who think about the value proposal for the next 18 months, work together with customers and orchestrate the concept to the point of launch. Crucially, these people don't have direct pressure from short-term sales figures, he notes.

For Turkcell CMO Ismail Bütün there are two schools of thought on marketing. Some believe marketing does a really important job, like that of a psychologist, he says. "You change the minds of people, buying behaviour, you influence people's behaviour," he explains. But others think "it's useless, it doesn't work, it's a waste of money". Marketing is about creating future value in the form of an intangible asset, the brand, he adds. "There are many compartments on a train but the locomotive should be the marketing," he says.

Malleschitz asks Bütün how telcos can ensure that this train follows the right course. Bütün responds that alignment in the company is "crucial" so that departments are all going in the same direction. "This focuses everything in marketing", he claims.

The goal is to communicate to finance-focused people that they need to create value not just today but tomorrow, according to Bütün. He says people "don't care" where they get electricity from but thinks Turkcell "means something" to customers. "There should be a story behind [the service] and that should be created by marketing," he notes.

What advice can the participants give to other CMOs about how to make marketing more of a priority at board level, Smith asks. Malleschitz says marketers need to make clear to the board what marketers actually do and tackle the

> "The whole industry sucks but we were the worst"

perception that marketers are "the fancy guys… hiring a celebrity, sitting on the set, sipping champagne, spending millions on a commercial no-one can prove the payback for". He hastens to clarify that "this is not marketing – there may be some haters creating these pictures".

Rather, Malleschitz says marketing is about what the company is standing for, what its proposition is and more fundamentally what its purpose is. "At the end of the day we are selling invisible connectivity, that's not really very exciting. It's a very real problem," he adds, noting UK telcos are less loved by customers than frozen food brands and less trusted than banks.

Another key goal is to build a relationship with the CFO, proving the benefits in terms of reducing churn for example. While it may take patience, Malleschitz says, relationships with the CFO help to get rid of the myths and explain the value of marketing.

For operators with a financially oriented CEO, meanwhile, Crucq says it is about starting from a consumer story and directly translating this into a business objective with a clear RoI.

We rip customers off all the time

Turkcell's Bütün has been in his role just under two years and is one of a number of telco CMOs to have arrived from a different industry. The CMO joined from the fast-moving consumer goods (FMCG) segment, where he worked as General Manager of the Beverages Group at Nestlé. There are similarities and dissimilarities between the two sectors, he says: in FMCG, the connection is far more fleeting – you simply put the Nescafé product in your basket and leave the supermarket, Bütün says. He adds: "Here in this industry you know your customer by heart." Telco customers in Turkey give their provider their ID, mean-

ing the telco knows everything about them, including their daily movements, and can offer services such as music or TV based on their behaviour.

But this close relationship throws up challenges. Bütün notes that telecoms customers expect constant service 24 hours a day, seven days a week. The structure of the campaigns is also different – telecoms run 30 campaigns throughout the 52 weeks of the year compared to the three or four focused periods typical to FMCG.

Bütün says he has brought some best practice over from FMCG – all members of the marketing team are expected to spend a day "in the field" at a call centre or store to "get closer to the customer", for example. But the rules of the game are changing, according to Bütün, with the telecoms industry facing not only internal competition but external threats from the OTT world of Facebook, Google and other apps. For "the time being", Bütün says, he does not regret his move to the telecoms industry.

Malleschitz concurs with Bütün on the faster-moving environment of telecoms: "It's three, four or five guys, plus maybe MVNOs, fighting for the same customer, still selling a utility trying to make more out of it," he says. A CMO must not only have a close relationship with the CFO but also understand what's happening "out there" in the market, Malleschitz adds.

He says he gets a "lot of energy back" from Three's in-store teams, who try to give him tasks using their systems to show how difficult their jobs are. It is easy to lose touch when the salaries in the operator's HQ are so much higher than those of the average citizen, Malleschitz notes, and speaking to employees helps to bridge this divide.

Kester Mann, Principal Analyst at CCS Insight, picks up Malleschitz's earlier point about the low reputation of the telecoms industry among consumers, saying that this area has been neglected by operators. Malleschitz says that while telcos are trusted in terms of handling finance and billing data, consumers don't feel a strong connection for the brand, and rightly so. "We are ripping customers off all the time. We lure them with cheap deals, cheap monthly fees, then you go over your allowance, we don't tell you [and] then we charge you a fortune. So you create this perception in the market that we are not trustworthy because we are not telling you what it really costs, we are not sticking to our words."

> "Diversity is a very powerful tool we should all embrace"

New skills needed

To enable them to turn around these perceptions, and much more besides, telcos are looking to hire recruits with a range of new skills. Turkcell doesn't face a major problem in winning over younger recruits, Bütün claims, which he attributes in part to the operator's "power to try to shape the industry". Crucq says winning new talent is not an issue for Proximus either. The business is "exciting, it's about innovation, it's about daily life, it's a very dynamic market," he explains.

Malleschitz is more circumspect. He says Three faces a huge challenge from the amount of competition centred on London, which he describes as an "innovation hub" featuring the best creative agencies and best start-ups. The kind of candidates Three are after would not necessarily be interested in working for a telco, Malleschitz admits. It has had some success, however, and now boasts veterans of PayPal and Skype in its ranks. Two things helped: the operator embraced remote working, which opened up access to talent around the world, and offered staff a blank canvas in creating new businesses, as long as they deliver on the bottom line within five years.

At Telekom Slovenia, CMO and CCO Ranko Jelaca has faced his own issues in competing for talent with other industries. He recounts the story of an accelerator that brought him into contact with a "genius" developer. Jelaca offered him a job and a permanent contract, but the candidate wasn't keen on working "for" the operator. He insisted on the term "with you", Jelaca remembers.

So what skills do telco CMOs need today in order to succeed, Smith asks. Bütün highlights the need to be able to parse huge amounts of data. "Big data is important but big questions are more important," the Turkcell CMO says, especially if you are going to come up with meaningful propositions.

Malleschitz chips in with the qualities of "perseverance and fast learning". He paraphrases a quotation attributed to Charles Darwin: "It is not the strongest of the species that survives, but the one

that is most adaptable to change." Fast learners who can adapt are already halfway there, he says. But CMOs also need to set the direction and inspire belief.

Crucq says it is getting more difficult to be a good marketer. As opposed to the time when brands were strong and people were choosing brands to belong to a group of people, it is now the opposite. Brands are required to adapt to any individual. They face the twin challenges of being relevant and authentic. This means going back to basics, Crucq says, co-creating with customers to bring them into the design phase of products and services. He warns against market surveys, which are slow to collate and end up with a product that may already be outdated.

The Proximus CMO thinks that everything should be designed to fit on the smartphone because "convenience is really the new loyalty". He also believes that CMOs need to be capable of content marketing, which is "not about the product itself, [but] about putting a spotlight on the experience and the emotions of experience that you can have as a customer." Crucq adds that CMOs need to be able to reach across silos, translating a consumer need into a viable business model and then bringing a telco's other operations behind it. This also means pre-empting internal opposition and winning over employees to the strategy, he says.

He also highlights the need to both react and adapt to short-term changes in the market while anticipating future trends. "[The] temptation to diverge from the strategy to attain short term tactical goals is frequent," Crucq adds.

Jelaca says CMOs need to be "very open" as people and says having experience of both B2B and B2C markets is an advantage. Interestingly, Jelaca says he uses more of the skills he learnt in B2B than those he learnt in B2C in his current role. He also talks of the importance of understanding that a brand is not simply a product but also a service, using the example of the quicker transactions that supermarket chain Lidl has managed to turn into a USP.

Most crucially, though, Jelaca says marketers should be good at spotting "basic human needs". While the way that consumers buy products and interact has changed, the needs that they are trying to fulfill have not, he claims.

Smith draws attention to the attendance of the roundtable – all middle-aged men. Is diversity something that requires more focus? Malleschitz, Crucq and Bütün all say that their marketing teams are predominantly female, but that there is less diversity in the other parts of the organisation. Jelaca says his organisation's management is now 70 percent women, including the Marketing Director.

Crucq says he tries to make his 90-person team representative of Belgium as a whole, in terms of Flemish and French speakers, young, mature, male and female. Malleschitz agrees that the voice of the customer is important and it's good to mix different types of people. "Diversity is a very powerful tool we should all embrace," he says.

However, Bütün is more sceptical of the idea that teams need to reflect their markets. It is more important that you have the ability to connect with customers, whatever age or sex you are, he says.

Reinventing the brand

Telekom Slovenia's Jelaca is the only participant who attended this same event in 2016. Last year, the CMO spoke about a goal he had of injecting more of a "hunter instinct" into the sales and marketing teams at the operator. Has he succeeded? "I think in some cases yes and some cases no," he responds. Jelaca highlights Telekom Slovenia's better performance in selling new connections, especially fixed, where acquisition of new customers more than doubled. The operator has also made good progress in its plans to pursue new business, including building its own set-top boxes and technology for connecting financial services.

In mobile, though, the company has been mired in a price war that started in May. Plans dropped in value from 10GB for €20 to 15GB for €13, leading to a decline in ARPU. "I think we are able to do it but I'm not sure that market performance can sustain the hunter instinct currently," Jelaca laments.

Crucq suggests two brands might be one way for CMOs to tackle price sensitive markets. The Belgian operator offers a no-frills brand called Scarlet alongside its main Proximus marque. Three and Turkcell have both taken a similar path.

Malleschitz says Three, which launched a low cost sub-brand called Smarty in August, has "unfinished business" with its main brand after the proposed merger with rival O2 was blocked by the European Commission in May 2016. The company has always claimed to be the brand for "disruptive" propositions, and

this remains a goal, says Malleschitz. But because Three is what its CDO calls a "Marmite" brand – in reference to the UK condiment which people supposedly either love or hate – Smarty was launched to cater for customer segments that Three is failing to connect with.

Turkcell, meanwhile, launched Lifecell in September 2017. This is a tariff that does not include minutes or SMS messages, instead carrying all calls and message as data traffic. Lifecell comes bundled with digital services, such as music and TV apps, as well as dedicated data for some social media sites.

Bütün says Turkcell wants to become a service or experience provider, offering a range of different apps, rather than a network provider. "We have so many babies to feed," he says. "[Turkcell] used to be only one brand, now it is seven."

Anthony Kendall, Strategy Director at Brand Finance, wonders whether the decision of many operators to launch new brands is the right one. "The external environment is already pretty challenging," he says. "Your response seems to be to create more brands, and that's a challenge in itself." Kendall notes that the usual tactic is to establish a good core brand and launch products off the back of it. Malleschitz counters that in order to reach all of the consumers in a market like the UK, "you have to branch out".

The roundtable is taking place just days after Vodafone unveiled a new global brand strategy under the "Future is Exciting" strapline. Its out-of-home advertising campaign aims to link mobile connectivity with pivotal moments in a subscriber's life such as organising a date. "It's almost like the telcos are the glue that holds all this exciting stuff together and yet they are not really getting the brand credit for that," says Kendall. But Malleschitz says that being the glue is "not good enough" and cites the example of one Three UK customer who got the operator's brand mascot Jackson tattooed on her ankle.

CCS Insight's Mann says the industry seems to be rather cyclical in its approach to branding. KPN in the Netherlands has scaled down from having five or six brands, he says, while BT operates three brands in the UK but faces questions on how the BT Mobile offering will be positioned against mobile arm EE. "One thing can't be all things to all people so you need to have those different segments," he says. But the flip side is that the more brands a company has, the more spending is needed, Mann adds. Bütün agrees: "For each period there is a right strategy. Sometimes more brands are needed, sometimes less. So there is no right or wrong, as long as it fits to your strategy."

Digital marketing and the quest for loyalty

Increasingly, telco CMOs are having to tackle the world of digital marketing. As customers migrate in ever greater numbers to social media channels and other online platforms, operators have scrabbling to understand how they can play in this area and engage with potentially new subscribers. Proximus is currently undertaking a major programme to upskill staff to better understand platforms such as Facebook. But the shift is more fundamental than just acquiring skills, Crucq says, requiring a move to digital-first from digital being an adjunct to the main marketing campaign. It requires "different kinds of formats, much more video, a different tone of voice" to other platforms, he says.

For the first time at this roundtable, Malleschitz appears conflicted. On the one hand, Three spends a lot on digital advertising, but on the other, the CDO says he "hates" digital advertising as a consumer himself. "I think there is something completely wrong with advertising, if the ad industry doesn't fix it they will get deep trouble," he says. Malleschitz lists a litany of problems, including the targeting not working and the fact that advertising consumes battery power and data. Three itself aims to take a "story-first" approach and find the best mix of media that services this story. It also collaborates with the online players to work out how best their particular platforms could be used.

Jelaca is also something of a sceptic. Ten to 15 years ago, he says he was delighted by the high usage of Facebook and YouTube, but now thinks the market is overcrowded and "the original idea of internet marketing has just disappeared". Digital marketing, he thinks, is now more intrusive than "any TV or any billboard" ever, because it follows you wherever your smartphone goes. There is also an ambiguity in what constitutes success in this field – is a high number of hits good, for example?

Turkcell's Bütün isn't exactly evangelical about the potential of digital for marketers either: "You shouldn't exaggerate digital but you shouldn't not ignore it either." He acknowledges it is a part of life, especially for younger generations, but thinks it is wrong to separate digital and non-digital marketing. What social

media has done is turn consumers themselves into brands, says Bütün, because they all post their own content online. This point is picked up by Jelaca, who says consumers expect "genuine" content rather than content that is produced by big brands.

The other thing digital has changed for Bütün is the specificity of marketing to certain regions. "The borders have disappeared," he says, adding that this is good news for small brands, who have a chance to reach a wide number of people with as little as $10,000. In fact, he sometimes challenges his team to create a campaign with this sum of money. "Amazing things happen, you cannot imagine," Bütün says.

The Turkcell CMO moves onto the topic of loyalty, using the example of his barber, who he has gone to for the last 10 to 15 years. "The barber said he had been a Turkcell subscriber for 10 years, what would be his reward for his loyalty?" Bütün countered with the fact he had been going to this barber for just as long – did that mean he deserved a free haircut?

Malleschitz says it is the fault of the telcos themselves, who have educated customers to threaten to quit, in order to have their loyalty is rewarded with a better contract. Bütün agrees, lamenting the high expectations combined with the lack of financial value that subscribers ascribe to the service. Rather than pay for a roaming bundle worth a few euros a day, he says people would rather pay for a single coffee in Starbucks and use the Wi-Fi. To get around this, Bütün says he has eliminated cheaper deals aimed at winning new customers.

At Proximus, the approach to loyalty is also being reconsidered. Crucq says the economics of giving rewards to customers are not proven. Loyalty is something deeper, he says, "a feeling of being sure that you made the right choice by being the customer of a certain brand, because you really get what you expect from that brand." This is something that companies "cannot buy, something you earn, and it's really like delivering your promise," he adds.

> "You shouldn't exaggerate digital but you shouldn't not ignore it either"

Face-to-face interaction with customers via retail stores could be one opportunity for telcos, says Mann. The analyst mentions Orange's flagship store in Paris, which he dubs "the future of mobile retail". A big four-storey shop which focuses on "technology and engagement" rather than selling, Mann says it's an "expensive investment", but "a really interesting new area".

Non-telco services and the future of CMOs

The example of Orange, which has launched its mobile banking service, provides a segue to the topic of how operators can market non-traditional services. Mann says operators have the assets to move into new services in terms of customer base, distribution and branding. However, he also thinks it is unclear where things like Orange Bank will actually make money, due to pressure on their traditional services, they may need to address new areas.

Crucq says Proximus is not looking at banking but has conducted trials into the smart home area. It is also interested in becoming a player in the advertising value chain, the CMO says. Launching new services is not an easy matter though, and requires considerable focus that may take resources from other areas, he warns.

Malleschitz says he would "love" to see an operator make a lot of money from a non-telco service and says it may be time for Three to look ahead to new areas. Kendall thinks telcos have been "a little conservative" in tackling these areas.

As the roundtable draws to a close, the final question strikes at the bone. With Coca-Cola having ditched the role of CMO earlier this year, is the job of the participants in the room under threat? Bütün says marketers can't just create a beloved brand if they are to prosper, they also need to create "value, money, profitability". Malleschitz, rather bleakly, remarks that "nothing is safe", but says the essential role of a marketer – to understand customers and fulfil their desires – will not change, even if the job title or the specific responsibilities associated with it do. For example, he says it may come to require more financial knowledge or more operational execution in the future. The last word goes to Proximus' Crucq, who ends on a suitably positive note: "I think at Proximus [the CMO role] will evolve and I hope grow further."

Vodafone's V cautious consumer IoT debut

Vodafone made its long-awaited entry into the consumer IoT market in November, launching four services including the V-Bag, below, that tracks your luggage. It was joined by a security camera, a pet tracking device and a dongle for your car that calls the emergency services in the case of an accident.

GSMA MOBILE™ WORLD CONGRESS

BARCELONA 26 FEB-1 MAR 2018

#MWC18

Mobile now connects more than two-thirds of the world's population.

It fuels innovation and revolutionises industries; creating exciting opportunities in communities around the world while providing lifelines of hope and reducing inequality.

Join us in Barcelona for MWC 2018 to discover how mobile is Creating a Better Future... Today.

AN EVENT OF MOBILE WORLD CAPITAL™ BARCELONA

WWW.MOBILEWORLDCONGRESS.COM


Thinking strategically
about the future of roaming
Manage your roaming customer base
as a digital community
MOBILEUM
Artificial Intelligence for Telecoms
• GROW REVENUES
• INNOVATE BUSINESS MODELS
• ACCELERATE DIGITAL TRANSFORMATION