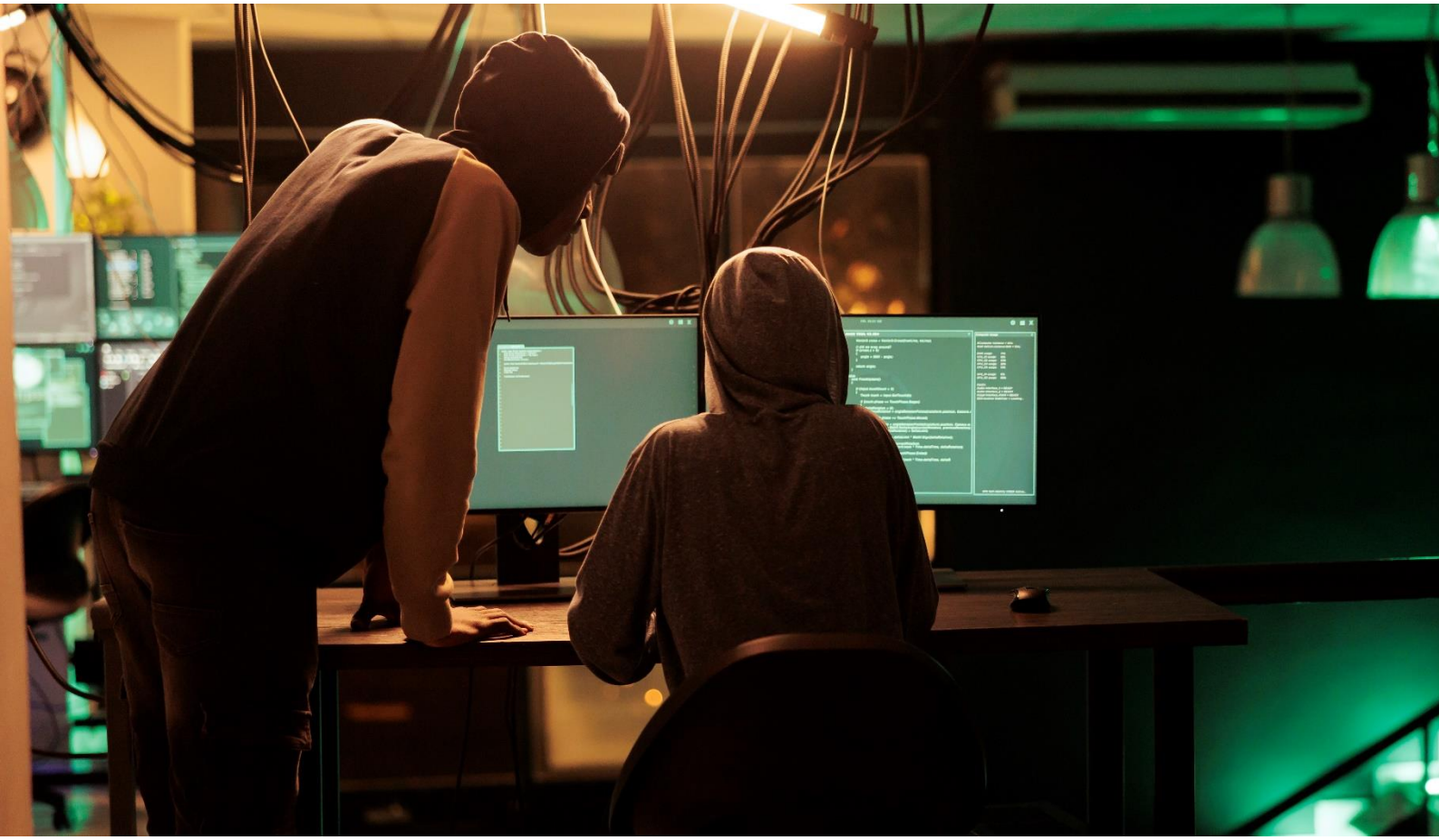

The cybersecurity opportunity for telcos

As artificial intelligence evolves, cyberattacks are becoming more sophisticated and costly for businesses. SMBs' cybersecurity needs are growing and becoming more complex, especially as companies adopt new technologies and ways of working. Telcos are in a strong position to increase their revenues and build longer-lasting relationships with their enterprise customers by offering them flexible, easy-to-deploy, end-to-end cybersecurity solutions.

Marina Koytcheva, Research Director

June 2024

Cybercrime is reaching new levels

I recently attended the Infosecurity Europe event in London (4-6 June 2024). As always at cybersecurity events, the progress of the "underworld" was a big topic, with spectacular examples; after all, this is the reason for the very existence of the cybersecurity companies in the first place. We all know that cybercriminals are not sleeping, but the speed at which they embrace new technology is astonishing.

I saw a demo of how a realistic deepfake video can be created quickly and easily with the help of a $10 app. Social engineering has reached new levels, with a multi-layer approach to individuals and businesses: for example, criminals target an individual personally, and once they steal their personal data, they blackmail the victim into disclosing company information or giving access to business systems.

And of course, cybercriminals now use artificial intelligence (AI). The days when spelling mistakes and bad grammar made a scam text message or email easily identifiable are ending. With generative AI, bad actors can create emails with the right tone and perfectly written in multiple languages.

Cybercriminals also have access to open-source large language models (LLMs). Cybersecurity experts claim that with help from the "dark side" criminals have even learned how to surpass the protective layers of "good AI" and use it to generate hacking code.

Businesses' need for cybersecurity is growing and getting more complex

Some small and medium businesses (SMBs) might have felt sheltered from big cybercrime, as the bad actors had larger fish to fry. However, the democratisation of generative AI is changing this.

Using LLMs, scam messages can be deeply customised to target many individuals and businesses with limited effort, so the pool of targets is likely to increase.

Another important factor is that as individuals and businesses keenly adopt the likes of ChatGPT, the risks to the security of a company's data, systems and intellectual property are not well understood. Employees may unknowingly expose information, which seems harmless, but AI can put pieces of a puzzle together and create a solid picture of the company if asked to do so by its competitors.

In addition, the cybersecurity needs of companies are becoming more complex as businesses adopt new technologies like cloud, and new network architectures like hybrid work or working from home. Bring-your-own-device practices, which have been widespread in SMBs for a while, are also bringing new challenges, as individuals start using AI on those devices for personal reasons, once again potentially exposing company data and systems.

Outsourcing cybersecurity may make sense for many SMBs

Big corporations have large teams focused on securing their data, business systems and AI models. However, smaller businesses often do not even have a dedicated IT person, let alone a cybersecurity professional.

At one of the keynotes, a data point was shared that 95% of the UK's SMBs have about half a person dedicated to cybersecurity, which is not surprising given the size of the businesses and the overall shortage of cybersecurity talent. As cybercrime becomes more sophisticated, so do cybersecurity solutions. Keeping up to date with new requirements, and even terminology, is not easy for employees whose main job is in another domain.

There are free learning resources available, including some government-sponsored, but they still require time to be invested in digesting them. SMBs may prefer to focus on winning in their own markets rather than spend time learning about cybersecurity and deciphering complex cybersecurity offerings.

Therefore, there is room for a trusted provider of end-to-end, flexible and affordable solutions to help SMBs acquire and deploy the right cybersecurity solutions.

Telcos have a role to play – if they want it

There is a clear role for telecom operators to provide those end-to end solutions to SMBs, possibly bundling them with connectivity or with other IT solutions, thus capturing a share of this growing market.

Many telcos have a significant headcount in cybersecurity. STL's Future Skills Tracker shows that on average cybersecurity professionals make up about 1.6% of telcos' headcount – more than the corresponding number in hyperscalers. Spark New Zealand, Singtel, BT, Elisa and Swisscom lead the way with significant recent investment in these skills.

In addition, telcos enjoy credibility in the cybersecurity industry. They have access to vast amounts of data across their networks. This enables them to monitor and manage cybersecurity threats by identifying threat patterns and signals. Verizon and Orange are examples of telcos particularly well regarded in this respect.

Our telco clients ask us why SMBs would be willing to buy such solutions from telecom operators rather than directly from a cybersecurity firm. Well, for one, because there are so many of those firms. The cybersecurity market remains surprisingly fragmented, and finding your way through it requires time and effort.

But there are also many reasons why telcos might be chosen as cybersecurity partners by SMBs:

- Telcos are trusted partners with trusted brands. Being regulated provides additional assurance.
- They can position themselves as independent advisors by selling the solutions of multiple vendors. This means that for every deployment they can choose the one solution that would best fit an enterprise's needs.
- Their subscription-based models can be flexible and suited to the changing needs of SMBs.

Therefore, packaging sophisticated cybersecurity software and services, and reselling them as hassle-free plug-and-play solutions to SMBs, will address a clear need in a growing market.

But would cybersecurity firms work with telcos? Indeed, we see several of those firms looking for ways to establish partnerships. Some do not yet partner with telcos mostly because they have not got around to it – but they would love to. Many of these companies excel in building software but are not so good in go-to-market, especially in the SMB segment which has diverse needs. Partnerships can be a great way for them to grow in the currently crowded market.

Telcos looking for ways to engage further with their SMB clients and deliver high-value services should consider the cybersecurity opportunity.

Marina Koytcheva is a Research Director at STL Partners specialising in telco strategy, consumer services and sustainability.

Get in touch with the author to learn more

marina.koytcheva@stlpartners.com

Visit STL Partners' Executive Briefing Service Hub for more insights on how telcos can grow their business

https://stlpartners.com/telecoms-strategy/