No.49
April 2021

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Vodafone Business Makes Security Bets

In March, Vodafone Business shared an update on its Cloud and Security business. Andrzej Kawalec, Head of Security Portfolio, shared the cyber security strategy.

- Vodafone Business is finally making a respectable commitment to security services.
- The company is leaning heavily on third party partners for its portfolio. Its own, internally developed, CyberHUB product will appeal most to very small businesses.
- Vodafone Business' commitment to simplifying cyber security will be very well received but too much simplification risks dumbing down and that must be avoided.
- The goal of trebling security revenues by 2025 looks achievable. That, in turn, suggests a sustainable, long term commitment to the cyber security market.

A Commitment That's Been a Long Time Coming

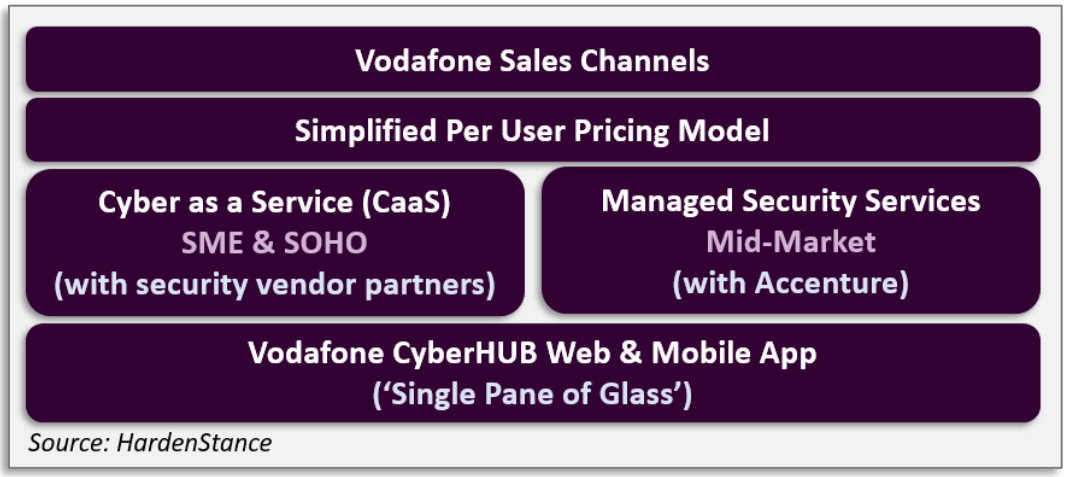
Of all the big European telcos, Vodafone has been the slowest to decide what to do about cyber security for business customers. There's a reason for that. While Vodafone Business does serve some large enterprises and multinationals with fixed telecoms services, the company isn't a fixed line services incumbent like Deutsche Telekom, BT or Orange. Hence it is not subjected to demands for high end enterprise security on a par with peers whose heritage dates back to being incumbent PTTs.

Of all the big European telcos, Vodafone Business has been the slowest to decide what to do about the market in cyber security for business customers.

Investing in its own MSSP Business Has Never Appealed

For this reason, Vodafone Business has always been reluctant to invest in its own large scale MSSP business against the likes of IBM Security, Secureworks or other large telco competitors. Instead, the strategy going back at least three or four years – probably longer – has focused on the need to serve the mid-market and SME sectors. But even with this more focused strategy, Vodafone Business has taken too long to deliver. As recently as two years ago, the best thing coming out of Vodafone in business security services was Secure Mobile Office – nothing more than the bundling together of Mobile

Figure 1: Vodafone Business' New Cyber Security Portfolio



Source: HardenStance

Threat Defence (mobile device security from Lookout) and Vodafone Secure Device Manager (VSDM) with O365. Up until recently, Vodafone has essentially combined and resold a few tools that can plug a few specific security exposures. That's a long way from being a trusted partner helping to protect all of a customer's digital assets from all the primary cyber threats it faces.

Vodafone's Message is That it's 'In It to Win It'

The core message coming out of last month's analyst briefing from Vodafone Business' Head of Security Portfolio, Andrzej Kawalec, was that Vodafone Business is making a more ambitious play in the cyber security space now. The roll out of a new portfolio is already well underway. The portfolio and supporting proof-points certainly look much better aligned with a company of Vodafone's ambition in the digital services business.

Some Compelling Declarations of Intent

Vodafone Business' declarations of intent around a core theme of enabling "Digital Resilience in the Connected World' strike many of the right notes. Here are a few of the statements Kawalec made during the briefing:

- "It's our mission and goal to effect a credibility shift in how enterprise security is delivered to smaller organizations."
- "We are genuinely aiming to be an absolute market leader in this space. It's an area we identify as having very little credible global competition."
- "A compelling and disruptive customer experience will sit at the heart of Vodafone's security offer."
- "It becomes much more about our customers' users, their data, their business activity and operations, their supply chain, and much less about Vodafone as a telco just protecting their network."
- "The Vodafone value consists of being able to curate an end-to-end security portfolio that you can understand and consume; integration of the entire security management layer; and then translation to a customer's individual business needs."

Vodafone Business wants to treble its security revenues by 2025.

Such statements of intent are bolder than anything Vodafone Business has made before. They will certainly be well received by business customers. SMEs are poorly served by the cyber security industry? Check. A credibility shift is needed to serve them better? Check. To succeed, leading telcos should help businesses secure all their assets rather than just their network? Check. As a CEO, CISO or even just the individual in a small business that picks up responsibility for cyber security, what's not to like?

As shown below, Kawalec shared some early customer proof-points and some long term targets for the new strategy. They assume an initial focus on the company's primary European markets, with roll out potentially following in other selected markets.

- **Vodafone Business wants to treble its cyber security revenues by 2025.** In the markets it is targeting, the company sizes the total security services market at €4 billion in FY21 and predicts it will grow at a CAGR of 12%, reaching €6 billion in FY 2024. HardenStance has no direct insight at all into Vodafone Business' security revenues. What is clear is that incumbent European telco peers with long established enterprise security businesses are generating in the range of €500 million to €1 billion a year. Since Vodafone Business only has a small stake in the large enterprise security market, HardenStance estimates the company's 2020 number to be in the range of €60 - €120 million. If that is correct, then that would point to a revenue target in the range of €180 - €360 million in cyber security services by 2025.
- **The company wants to grow its customer base for cyber security services to 45,000 in the same four to five year time frame.** This represents quite a bit less than 10% of Vodafone's total base of SME and larger business customers world-

wide. However it's likely to represent quite a bit more than just 10% of these customers in Europe, where the large majority of security revenues can expect to be generated for at least the next year or two.

Vodafone's Business Model for Security Services

Whereas European telco peers have invested in their own MSSP businesses, Vodafone Business is taking the capex-light approach of depending on core security partners while serving as the channel, sales engagement and service management lead itself.

A lot of its market messaging focuses on simplifying cyber security. Consistent with that, its pricing model takes no account of a customer's numbers of devices, device types, or volume of data consumed. Moreover, there is no up-front fee. Instead, pricing is based on a simple price per-user rolled up into a monthly fee. This applies not just to SME and SOHO-tailored services but to complex managed services for the mid-market as well.

The Mid-Market Managed Service, Partnering Accenture

The sign that Vodafone Business was at last ready to make a move befitting a company of its size was last July's announcement that it would partner Accenture for managed security services in the mid-market – companies with advanced cyber security requirements but no intention of staffing up their own in-house cyber security team. This partnership was announced just three months after Accenture completed the acquisition of Symantec Cyber Security Services (CSS), the company's MSSP business.

The pricing model takes no account of a customer's numbers of devices, device types, or volume of data. There is no up-front fee. Instead, pricing is based on a price per-user aggregated up into a monthly fee.

This mid-market service, operated by Accenture, is already up and running in Italy and Spain. 50 customers signed up for at least one component of the service within three months. The UK and Germany are up next. Besides referring to it as the "massively ground-breaking" partnership with Accenture, Andrzej Kawalec didn't share much detail around the composition of the managed service except that Palo Alto Networks provides some of the foundational network security capabilities underpinning it.

The pitch suggests a pretty comprehensive service that covers all five of the NIST Cyber Security Framework domains of Identification; Protection; Detection; Response and Recovery. In other words, consistent with Vodafone's core messaging, the offer is a comprehensive one, positioned as a trusted end-to-end managed offer for everything from scoping risk at the front end to recovering from a breach at the back end.

CaaS for SME and SOHO Customers

For the SME and SOHO markets, Vodafone Business is offering Cyber as a Service (CaaS) propositions built around a principle that these customers should be able to 'Click to Understand', 'Click to Buy', 'Click to Consume' and 'Click to Manage'. These are based on vendor partners such as AON (risk assessment solutions);Trend Micro (endpoint web browsing, email security); and Lookout (mobile security). Services are available stand-alone or bundled in with telecom or other business services tariffs. Five CaaS services have been launched in the UK, the Netherlands, India, Spain and Italy. As of the middle of March, these had generated sales of 60,000 licences across 8,000 customers.

Vodafone's Own CyberHUB For Business Customers

Any telco wanting to be a substantial player in cyber security services wants to be seen by customers and partners as more than a front-end sales and back-end billing engine. Consistent with leading on the service management, Vodafone Business has therefore developed its 'CyberHUB' that will form part of Vodafone's V-Hub. This serves as a repository for businesses looking to exploit digital technologies.

Due to launch later in Q2 2021, CyberHUB is being positioned as "redefining how cyber security is consumed" by business customers. It offers a 'Single Pane of Glass' that provides summary visibility and status updates across the suite of security services delivered by Vodafone and its partners. CyberHUB can be accessed via the web as well as via a mobile app with a customizable GUI.

The CyberHUB looks much more likely to appeal to small customers than large ones. Not many CISOs in medium sized firms are going to sleep any easier just because their computer screen (let alone their smartphone) isn't currently flashing red. Moreover, the first iterations of the CyberHUB will only support Vodafone or Vodafone partner-supplied products and services. The ability to integrate a customer's other security products and services into CyberHUB isn't even a formal roadmap commitment at this point.

HardenStance's Take

HardenStance has three key take-aways as regards the outlook for the Vodafone Business strategy:

- The revenue targets are achievable – and that's encouraging.
- Managed Security is hard – 2021 and 2022 will be a 'Honeymoon Period'.
- Simplification matters but over-simplification presents its own risks.

The Revenue Targets are Achievable – and that's Encouraging

For any cyber security professional, the next couple of years look like a good time to be working with Vodafone Business – as an employee, vendor partner or a customer. When a big company takes too long to commit to a key product space, the wave of investment, management attention, sales and product development activity that eventually gets unleashed tends to create an infectious energy. This is what seems to be going on here. If HardenStance's estimate that 2020 cyber security revenues were in the €60 - €120 million range are correct, then trebling that number by 2025 doesn't look that tough a target. That's a good thing because achievable revenue targets imply that Vodafone Business has a sustainable, long term, commitment to the security space.

The success of any MSSP business stands or falls on how efficiently customer engagements are managed to deliver customer satisfaction while managing margins.

Managed Security is Hard – 2021 and 2022 will be a 'Honeymoon Period'

In the case of the mid-market managed services in particular, this next year or two will be a honeymoon period. But with managed services partnerships, an aggressive customer acquisition phase will inevitably be followed by a period of review to scrutinize customer satisfaction metrics, the impact on customer churn rates, and margin performance. That's when the viability of the business model will start to be proven - or not. After that pause and review comes the decision to either double down and grow again or cut back and re-trench.

The success of any MSSP business stands or falls on how efficiently customer engagements are managed to deliver customer satisfaction while managing margins. That boils down to things like prioritizing the automation of security workflow rather than call centre automation; aligning SOC analyst incentives with metrics that impact final outcomes as experienced by the customer (and the analyst) rather than internal benchmarks; as well as the quality of the talent retention program. Success or failure also turns on how well the provider is able to engage customers in understanding their own responsibilities for achieving target outcomes - and living up to them.

Via the acquisition of Symantec's MSSP business, Accenture will have access to a lot of experience that can point to how this can be done. However, it's not a given that Accenture's business culture will be willing – or even able – to act on that advice. The fortunes of Vodafone Business in this space are heavily dependent on Accenture getting this right – but there's not a lot Vodafone can do to influence that.

Simplification Matters but Over-Simplification Presents its own Risks

HardenStance recognizes and echoes the importance Vodafone Business attaches to simplifying cyber security. There's no doubt that the cyber security industry as a whole is too often guilty of compounding technology and process complexities and that attempts to simplify them are very welcome. But equally, there is a risk of messaging around simplification inadvertently encouraging complacency on the part of customers.

Engaging an MSSP could well require a customer organization as a whole to invest as much, if not more, of its own time on cyber security than it ever did previously. So as well as committing to taking complex problems off their hands so that they can concentrate on doing what they're good at, the best cyber security partners don't hesitate to tell customers – even demand from them – the changes that are required within their organizations if jointly-agreed cyber security goals are to be reached.

Consistent with committing to a responsible pitch around simplifying security, Vodafone Business needs to be mindful that it doesn't indulge or encourage customer complacency. Because committing to grappling with some amount of complexity and time-consuming drudgery is an inevitable and necessary part of good cyber security - whether a customer likes it or not.

More Information

- HardenStance Briefing: "Vodafone Targets SME with Security" (October 2018)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer