No.51
May 17th 2021

HardenStance Briefing

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

Of Course Singtel Should Sell Trustwave

- Trustwave was never a good fit but Singtel compounded flaws in the original strategy with decisions that may have set its positioning in cyber security back still further.
- The acquisition hasn't worked. Singtel should sell Trustwave and spend the proceeds on a cyber security strategy that's better aligned with its corporate strategy.
- Trustwave is a good asset for the right buyer. The prime candidates are the big accounting firms, cyber security companies, IT companies and U.S. telcos.

An Already-Flawed Strategy, Poorly Executed On

Friday's announcement by Singtel that it is considering the sale of Trustwave comes as no surprise. The only surprising thing is that it has taken so long. Back in April 2015, the rationale behind the estimated US$ 810 million acquisition was questioned by many analysts: why on earth would one of Asia's most advanced telcos want to buy an American Managed Security Service Provider (MSSP) with a big customer footprint in the United States, a growing one in Europe, but hardly any in Asia?

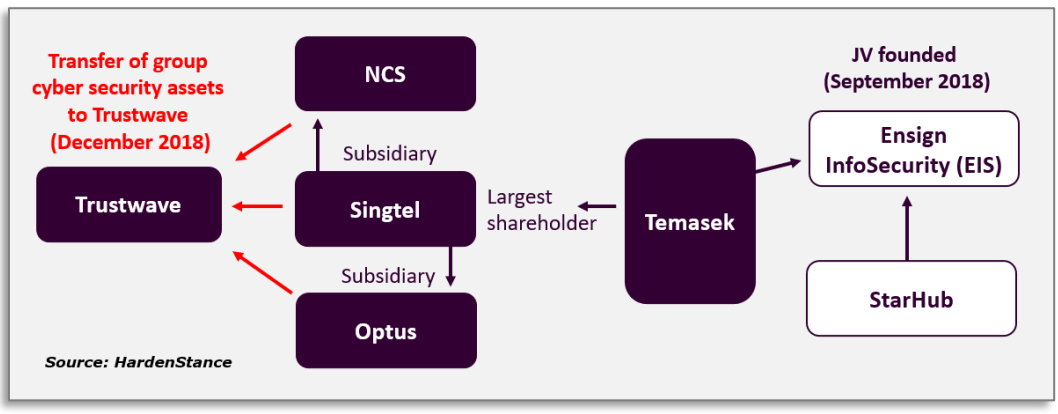
Trustwave's menu of standardized service packages was never a very good fit for the more custom needs of Singtel's core business market of government and large corporates.

That was always the right question - to which there has never been a satisfactory answer. The only way to construct a convincing strategic rationale for it was on the basis that synergies between parent and acquired asset would flow such that Singtel would grow its security capabilities to better serve its core customers. Trustwave would also replicate its MSSP win rate in the U.S. throughout Asia. Trustwave's business trajectory would also see it emerge from loss-making into profit.

Some Salutary Lessons for other Telcos

There are some salutary lessons here for other telcos looking to enter the MSSP market via M&A because precious little of this supposed promise appears to have materialized. From the outset the mismatch was more than just geographical. At least as much as most MSSPs – probably more so – Trustwave's core market is the mid-market. These are companies that are big enough to have complex cyber security requirements but they're not big enough to justify big investments in in-house cyber security operations.

Figure 1: Group Cyber Security Assets Were Transferred to Trustwave



In that sense, Trustwave's menu of standardized service packages was never a very good fit for the more custom needs of Singtel's core enterprise market of government and large corporates. Moreover, with many countries in the region lacking the data protection and cyber security regulations that are common in western countries, Asia wasn't as ripe for MSSP services as North America and Europe (arguably, it still isn't).

With hindsight, a key milestone in the unravelling of this unhappy marriage was the September 2018 founding of Ensign InfoSecurity (EIS), a cyber security JV between Temasek and StarHub targeting corporates and government organizations throughout Asia. This was significant because Temasek is Singtel's largest shareholder and StarHub is a key competitor of Singtel's. Were it not for disappointment at Trustwave's ability to serve this key market, it's debatable whether EIS would ever have been formed.

Singtel Doubled Down on its Errors

Singtel didn't just fail to correct Trustwave's misalignment with its corporate strategy- it actually doubled down on its errors. As shown in **Figure 1**, in December 2018 Singtel made the fateful decision to move all of the group's cyber security assets from Singtel and subsidiaries like Optus (Australia) and NCS (its IT and communications engineering company) into Trustwave. That's right, much of the company's own Systems Integrator (SI) and cyber security assets were transferred from those parts of Singtel that were aligned with corporate strategy to the part that wasn't. That must have made some kind of sense to the Board of Singtel - but it isn't likely to have made much sense to the company's enterprise sales teams engaging with customers on the ground.

Trustwave is a potentially good acquisition for the right company. It may well have under-achieved in Europe and North America in recent years.

It's unclear what – if any – repercussions this has been having on Singtel's core business. For example, no telco can succeed in the 5G enterprise market – whether that's built on private 5G networks or telco network slices – without a compelling suite of security services including managed security services.

Singtel customers have to hope that in the two and half years since that decision was made, some of the cyber security capabilities originally transferred to Trustwave have been either overtly or covertly 'clawed back' to the Singtel group's core telco businesses where they're most needed. If that hasn't happened, then Singtel and Optus may have lost ground in building 5G enterprise security portfolios to competitors like StarHub and M1 in Singapore and Telstra in Australia. These competitors have resisted making the same vanity M&A play in cyber security.

Notwithstanding the poor fit with Singtel, Trustwave is potentially a good acquisition for the right company. It may even have under-achieved in Europe and North America due to years of having to try to shoe-horn itself into a not very receptive Asian market and lacking effective support from its parent. The list of prospective buyers is likely to feature the usual suspects among IT companies, cyber security firms, big accounting firms as well as telcos (albeit those with a focus on North America or perhaps Europe).

Of course Singtel should sell Trustwave. It's been a bad fit from the outset. Singtel should then leverage the proceeds of the sale to bolster its cyber security competences – whether internally, through M&A, or a combination of the two. A new strategy has a much better chance of aligning with the demands of Singtel's core customers and geographies compared with trying to somehow turn the Trustwave ship around. That ship has sailed – and it's not coming back. ■

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

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.