THE BUSINESS TIMES

S$1.30 SPH A SINGAPORE PRESS HOLDINGS PUBLICATION | businesstimes.com.sg | fb.com/thebusinesstimes | @BusinessTimes | CO REGN NO 198402868E | MCI (P) 048/12/2018 Tuesday, July 16, 2019

TRADE WAR WOES
China's economy sputters with 6.2% growth in Q2
TOP STORIES / 4

KEY WORKS
Willowmore's smart locks are robust enough for industrial use SME / 28

FINANCIAL WELLNESS INDEX
Most working adults not financially ready for retirement TOP STORIES / 2

HOCK LOCK SIEW
Sentosa Cove in need of a boost in profile
COMPANIES & MARKETS / 8

MARKETS

	Monday	Change
STI	3,347.95	-9.39
KL COMP	1,672.37	+2.92
NIKKEI 225	CLOSED	–
HANG SENG	28,554.88	+83.26
SHENZHEN B	979.74	+0.43
DOW (11am EST)	27,333.72	+1.69

GROWING dependence on technology has led to many concerns about its security: Hacking and phishing are just a couple of well-known ways our data can be compromised.

Another issue, which may not seem linked to security on the surface, is the chaos that ensues when telecommunications services are disrupted. Yet, security plays a part here too - some of the difficulties in restoring service stem from the system of physical locks used to secure telecoms sites located around Singapore.

Telco staff must retrieve physical keys in order to access the sites and restore service, prolonging the disruptions. Keys also are easy to duplicate and mechanical locks could be accidentally left unlocked, leading to theft and tampering.

Smart lock solutions company Willowmore was born from the discovery of such issues with current security solutions, which co-founders and managing partners Basil Byrne and Joseph Tey uncovered in their consulting work for telecoms companies.

Over two years, Willowmore developed a keyless smart lock system that allows enterprises to issue virtual keys quickly to the smartphones of authorised staff and contractors, while simultaneously ensuring their distributed assets are secured and every entry is tracked.

While other smart lock systems exist, many are meant for consumer use and therefore are not as robust as needed for enterprises, Mr Byrne told The Business Times. For instance, because radio signals cannot pass through steel, most smart locks would contain a plastic element, weakening the lock.

Willowmore developed an industrial-grade stainless steel lock that can still transmit radio signals, ensuring that it is strong enough to withstand physical damage while still being able to connect wirelessly to the monitoring system.

"We're very confident that the lock business will be successful, because pretty much every mechanical lock in the world is going to have to be changed," Mr Byrne said. He added that while Willowmore has targeted mainly telcos with its solution so far, such smart locks would be useful for any company with distributed assets.

He cited the rise of 3D printing as a modern threat to security, since keys can be duplicated at a fraction of the usual cost and time, while the sharing economy has resulted in the need for multiple individuals to access the same assets.

Already, sites such as Housing Development Board rooftops house utilities equipment alongside telco assets, and 5G networks in future will have infrastructure scattered around the country, which will need to be shared among telcos as well.

"There might be three operators wanting to access one asset. You're worried about your competitors going in, and you have no idea what's going on. (With smart locks) if somebody goes in and brings the site down, you know exactly who did it."

Mr Byrne added: "With mechanical locks, companies have no idea whether their assets are secure. They have S$100,000 in assets sitting there, and they just really hope the subcontractor locked it. If you had a S$100,000 car, you probably wouldn't want somebody to 'hope they locked it'."

Willowmore doesn't see itself as a lock company, but more as a data company, because it plans to leverage a wealth of data to secure sites and improve efficiency beyond the abilities of physical locks.

After one of Willowmore's major clients in Indonesia implemented its smart lock system, the data showed that 6 per cent of the client's sites were never locked, because workers had developed a habit of leaving the sites unsecured to avoid extra trips to return and retrieve the keys daily.

This discovery would never have been made with the traditional mechanical padlock system, Mr Byrne pointed out.

Customers will soon be able to monitor other factors such as temperature and movement with inexpensive, but reliable Bluetooth chips to detect overheating problems or break-ins. Willowmore has developed a patent-pending gateway for the next iteration of its lock, which will use Bluetooth technology to connect with sensors on-site, and the more expensive Internet of Things (IoT) technology to send alerts to the asset owner even when power grids or telco service fails.

Eventually, Willowmore plans to overlay third-party data such as weather and traffic information onto its system, which would help companies avoid sending maintenance workers out into traffic jams or bad weather, for instance.

The company is almost fully self-funded, with one angel investor holding a 10 per cent stake, while the remaining 90 per cent ownership is split between the two co-founders.

The lock business has grown to account for nearly half of Willowmore's revenue of S$2 million and most of their team of about 25, with the consulting business making up the rest of the revenue and employing a handful of its workforce.

Mr Byrne said Willowmore will likely continue to offer consulting services even as the lock business grows, since it helps the company remain self-funded and keeps the team abreast of the latest developments in the telecoms industry.

He is optimistic that Willowmore's customer base will swell as the company engages with business leaders in various industries to convince them of the need for smart locks to combat modern security threats.

Its smart lock solution has already been evaluated by the GSM Association - a trade body representing mobile network operators worldwide - and listed among other case studies of solutions focused on areas for operators to potentially reduce operational and capital expenditure.

The company has also conducted extensive trials in South-east Asia and collected references from companies in Singapore, Indonesia, Thailand and Australia, among others, and will use these to demonstrate its solution's effectiveness.

"We would love to have smart locks on every piece of infrastructure in this country. Even if it's not using our product, it should be done," Mr Byrne said.

"We should not be using stuff designed a hundred years ago. We want to work with the Smart Nation concept and help protect assets and critical infrastructure, and do it with smart technology."

This article was first published on www.sgsme.sg