Group Enterprise

For most businesses today, a strong online presence is a prerequisite for success. Singtel provides enterprises with global connectivity 24/7 by harnessing the powers of our core ICT services while our focus on cyber security keeps out unwanted connections. We have also been expanding our cloud capabilities and devising smart city solutions to help government agencies and companies in their own digital transformation. Starting out small? You can still dream big with our raft of initiatives to encourage technology adoption and networking opportunities that cater to the needs of small and medium businesses.

LOW FANG LING

Sales Manager, Group Enterprise

Wei Chan, the CEO of Pine Garden, dreams of turning his family-run chain of cake shops into what he calls "new old-school bakeries". After learning about the 99%SME programme, which helps small businesses to maximise their online potential, he placed promotions of his fresh cream cakes on its website and was pleased with the exposure. Fang Ling is encouraged by his experience, and eagerly shares with other SMEs the benefits of expanding their customer base by moving online and tapping into the power of e-commerce.

Group Enterprise

Today's enterprises and governments are adopting secure, high-speed unified communications, mobility and digital solutions to improve the way they operate and engage with their customers in the digital economy. Singtel is building successful partnerships with enterprises, large and small, to support their digital transformation through our core ICT services and strategic focus areas of cloud, cyber security and smart city solutions.

STRENGTHENING OUR CORE ICT CAPABILITIES

As ICT traffic grows, we continue to invest in building out and enhancing our networks to deliver seamless, high-speed global connectivity to our customers.

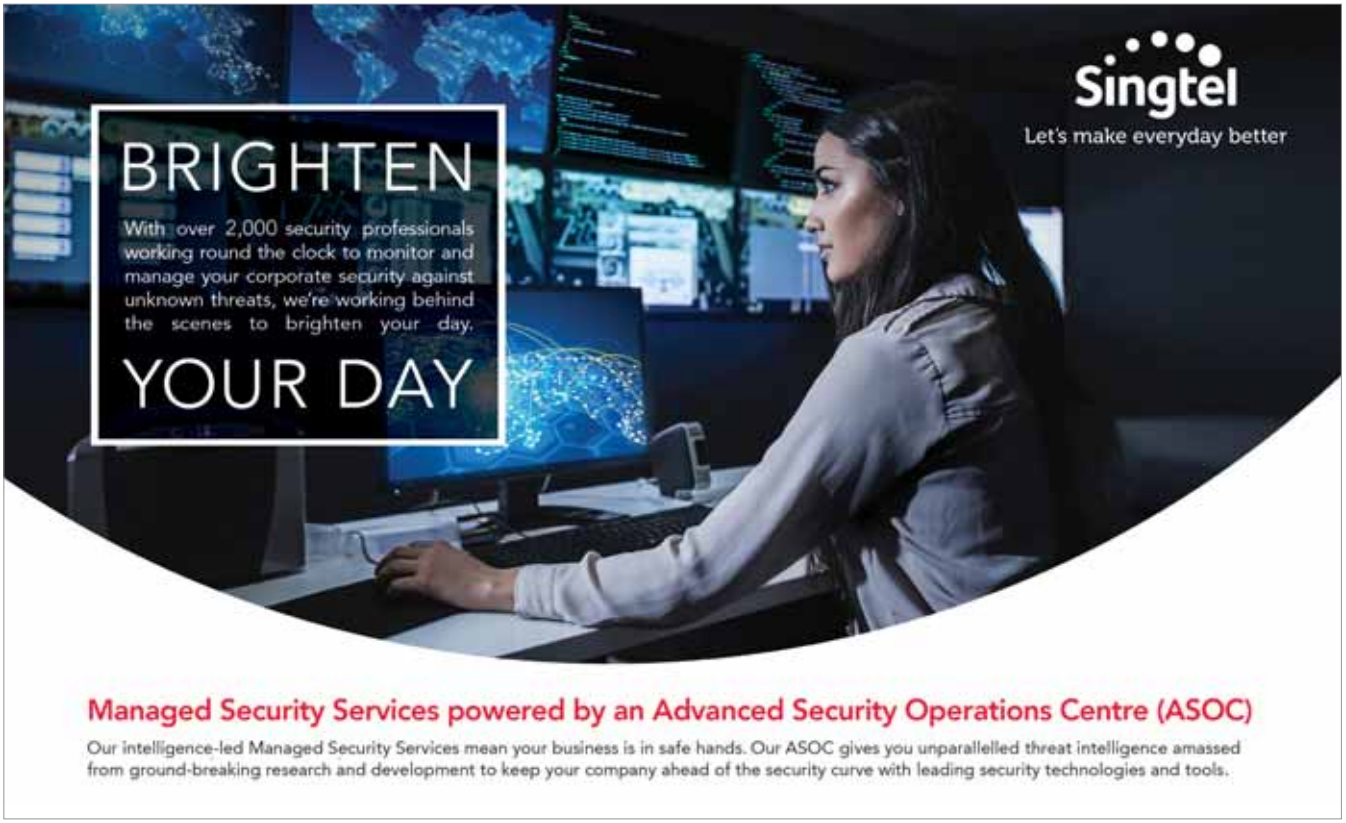
We expanded our global coverage to 370 points of presence in 325 cities across the world through a partnership with our regional associate, Airtel.

The combined network is the largest Internet Protocol Virtual Private Network (IP VPN) in the Asia Pacific.

We are also leading a consortium to build a new 9,000-kilometre INDIGO submarine cable (formerly known as APX-West) linking Singapore, Jakarta (Indonesia), and Perth and Sydney (Australia). Once completed in mid-2019, it will expand data connectivity and capacity between Singapore and Australia, providing network redundancy and low latency. This will allow us to meet the growing demand for bandwidth-intensive applications such as unified communications and enterprise data exchange.

EXPANDING OUR CLOUD SERVICES

The demand for cloud services is steadily growing as enterprises seek to transform their business processes and models for the speed, agility and efficiency that they need in today's digital economy.



What the media said

"Over the past few years, Singtel has also been very shrewd in investing in a bunch of cyber security companies, the latest being Trustwave, and making alliances with others. This has already had a positive impact on its Group Enterprise business and this impact will only grow." – Amit Choudhury, The Business Times

We added a suite of hybrid cloud solutions, including the Data Centre and Cloud Connect (DC Connect) service, to cater to enterprises requiring both the easy scalability afforded by the public cloud, and the improved security and control of a private cloud. With DC Connect, enterprises can easily access and seamlessly move their workloads between multiple data centres and various cloud services through a single connection. This enables them to build a hybrid cloud environment where they can shift the mix between public and private clouds according to their business priorities.

BOLSTERING OUR CYBER SECURITY EXPERTISE

As enterprises and governments transform themselves in the digital space, they also need to protect themselves against cyber threats which are growing in frequency and sophistication.

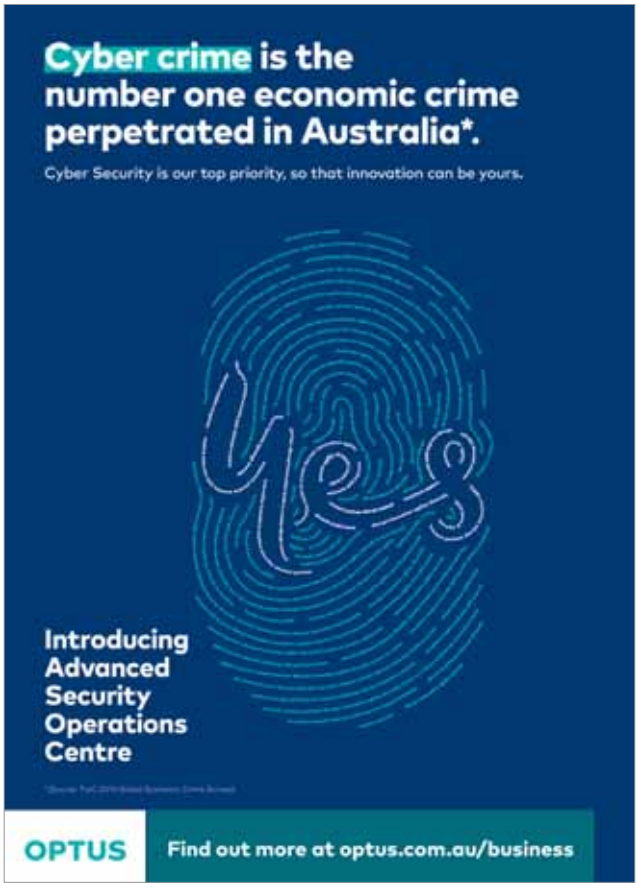
In the past year, we focused on developing a comprehensive cyber ecosystem by strengthening our cyber expertise and expanding our global cyber network.

We established the NUS-Singtel Cyber Security R&D Lab with the National University of Singapore. This collaboration allows us to conduct research into next-generation cyber security technologies which are based on data analytics, machine learning for automatic detection of cyber attacks, and tamper-proof encryption techniques over the next five years. The facility, which is supported by the National Research Foundation, will train 120 new cyber security R&D

Group Enterprise

professionals from undergraduate to postdoctoral level. It will also develop intellectual property that can be commercialised through our global network of product engineering and development centres.

We launched the Optus Advanced Security Operations Centre (ASOC) in Sydney, Australia, and we will soon operate a new ASOC in Tokyo, Japan. The two centres add to our existing global network of seven ASOCs which monitor cyber threats round the clock, help enterprises build cyber resilience and protect their critical infrastructure. Trustwave, our cyber security arm, provides managed security services, including comprehensive threat intelligence, threat data analytics, and advanced security automation for incident response, backed by its elite SpiderLabs team. We also partnered our regional associate Globe to provide managed security services in the Philippines. The services will be delivered through Globe's ASOC in Manila, which will be powered by Trustwave.



We set up the Singtel Cyber Security Institute in Singapore. Our advanced cyber range and educational institute is the first of its kind in the region to provide holistic training for company boards, management, and technology and operations personnel to deal with cyber attacks.

ENABLING THE SMART CITY VISION

As cities grow, city planners increasingly recognise that cities need to be smart and sustainable to overcome the attendant environmental, economic and social challenges. They rely on smart technology solutions for the efficient and effective delivery of public services, better traffic management, and a safer home and living environment.

In Singapore, we support the country's vision of becoming the world's first Smart Nation by 2025 with our advanced capabilities in smart city operating platforms, data analytics and agile application development. These capabilities are being deployed in a number of

What the media said

"In the last two years, Singtel has accelerated efforts to grow the business – securing partnerships with global big names, and launching new facilities in cyber security. It is approaching the field of cyber security in trailblazer fashion."
– Jacquelyn Cheok, The Business Times

What the media said

"SMEs in Singapore are getting a little digital love from DBS Bank and major telco Singtel ... they're launching a bunch of resources meant to help small businesses with e-commerce and cashless payments." – Michael Tegos, TechInAsia

areas, including urban infrastructure, transport, healthcare and public safety.

Following our winning bid in early 2016 to deliver a next-generation Electronic Road Pricing system for the Land Transport Authority, we scored a significant contract with the Housing & Development Board (HDB) to develop a blueprint for smart HDB towns of the future under the Smart Urban Habitat Masterplan, and a Smart Hub intelligent analytics and data platform. With more than 80% of Singapore's population living in public housing, this will help the HDB to enhance the planning, design and management of public housing estates, to create a more conducive and sustainable urban environment.

In Australia, we are rolling out smart retail WiFi services at Vicinity Centres' 81 shopping centres and six corporate offices, as well as property group Mirvac's flagship shopping centres. More than 120 major malls now use these services to deliver personalised content and improve the shopping experience for their customers.

EQUIPPING SMEs IN THE DIGITAL ECONOMY

Small and medium enterprises (SMEs) are the bedrock of the Singapore economy, accounting for 99% of all registered businesses. To help SMEs evolve and connect with increasingly digital-savvy consumers, we launched 99%SME in 2015, a five-year campaign to spur the adoption of digital technologies. Digitalisation will enable SMEs to increase productivity, reduce staff workload, improve customer experience and reach new customers.

The second year of the campaign focused on encouraging SMEs to adopt e-commerce and cashless solutions. More than 2,500 SMEs signed up in 2016, up from 1,670 in 2015. The campaign rallied consumers across Singapore to buy SME products and services through year-round promotions on the dedicated 99%SME website and shop at participating stores during a 10-day 99%SME Week.

We partnered online shopping website Lazada Singapore to launch a 99%SME e-marketplace, which provides SMEs with an online marketing platform to reach a wider audience. We also collaborated with two polytechnics in Singapore – Nanyang Polytechnic and Singapore Polytechnic – to train SMEs in the retail and food and beverage sectors to use tools and resources to get online, establish e-commerce capabilities and to market themselves more effectively.

The CEO Conversation

BILL CHANG
CEO, GROUP ENTERPRISE

Why cyber security is a must-have

With cyber attacks on the rise, what can companies do to protect themselves and their assets? We talk to Group Enterprise CEO Bill Chang about overcoming today's security challenges.

Incidents of cyber attacks are well-reported, but far less is known about how companies can defend themselves. What should they be doing?

Bill: Almost every day, the media uncovers a new massive data breach or cyber security incident. Most cyber attacks involve cross-border criminal activities and can take place anytime. So it's really a question of when a cyber breach will occur, not if.

While everyone accepts this, many companies still don't quite know where to start in terms of protecting themselves and are simply not doing enough. In fact, many are still leaving cyber security to their technical staff. We believe leadership from the top is essential. Everyone needs to know what the risks are and what they should do to manage risk effectively. A lot is at stake here. Cyber breaches can affect operations, cause the loss of intellectual property or market-sensitive information, reputation and even enterprise value.

How should company leaders get involved?

Bill: For starters, board members have to work closely with top management to understand the value of the company's data, the associated risks and impact of losing key data within their overall enterprise risk management framework. They also need to understand how their data is being protected and who has access to it. This way, they can make accurate cyber risk assessments and implement appropriate defence strategies.

Next, they should assess cyber security capabilities within the company to ensure there is enough bench strength to mitigate the cyber risks. The reality is few boards and management have such expertise.

Are there training sessions that can help build up such expertise?

Bill: Yes. Company leaders need to invest in training in areas such as risk assessment and mitigation. They also need training in crisis management and communications, which are crucial in today's world of instant news and active social media.

But classroom training can only do so much. You need highly realistic simulations where board members, C-suites and technical staff are made to work together to manage

"Everyone needs to know what the risks are and what they should do to manage risk effectively. A lot is at stake here. Cyber breaches can affect operations, cause the loss of intellectual property or market-sensitive information, reputation and even enterprise value."

BILL CHANG
CEO, GROUP ENTERPRISE

a cyber incident. This is the true test of a company's cyber preparedness. We've been conducting such simulations at the Singtel Cyber Security Institute, which was set up to educate and train companies to better handle cyber breach incidents.

How do they foster cyber security awareness among their staff too?

Bill: Cyber resilience requires active participation by all members of staff. Company directors and top management need to create a culture of cyber preparedness and sound security practices. Given how quickly cyber threats evolve, they also need to regularly review and update their cyber defence strategies across all levels of their operations. This means ensuring adequate funding and resources to support such strategies.

Top management should also examine their organisations' supply chain, to assess the cyber risk posed by their contractors and suppliers. The negligence and lapses of supply chains have been known to contribute to serious breaches as well.

What about companies that lack the resources to focus on cyber capabilities?

Bill: With cyber threats increasing in frequency, scale and sophistication, the reality is no single company or country can address these cyber threats alone. Many companies also lack the manpower to maintain an effective 24/7 cyber defence. The good news is, they can tap on the resources and capabilities of credible managed security services providers (MSSPs) that are global, have highly-trained cyber security professionals and offer real-time intelligence on cyber threats.

MSSPs themselves collaborate with global providers of cyber security technology solutions. This gives companies the convenience of dealing with only one party instead of multiple providers, each offering its solution to only one particular form of cyber threat.

This trend of engaging MSSPs has already caught on globally. We have seen more and more companies taking up partnerships with cyber security firms to install, monitor and maintain their cyber defence systems. Singtel's cyber security arm, Trustwave, has reported that the number of companies worldwide that are partnering MSSPs has risen from 24% in 2015 to 33% in 2017.

What other services can managed security services providers provide companies with?

Bill: Our cyber security solutions and services cover everything a company needs before, during and after a cyber breach. Managed advanced threat prevention and threat protection for a comprehensive range of endpoint devices and DDoS protection are just some of the solutions we offer. Our services include cyber security readiness assessment, vulnerability and penetration testing, incident response and forensic investigation.

The cyber security industry as a whole is facing a shortage of trained professionals. What can companies do if they need staff in this area?

Bill: It's true that there is a severe shortage of trained cyber security professionals around the world, not just in Singapore. Some ways to address this is to retrain mid-career IT staff in cyber security, or partner institutions of higher learning to sponsor students in cyber security studies. They can also provide internship opportunities.

But the grooming process takes time. Singtel has been working closely with various government agencies and educational institutions to boost our force of more than 2,000 cyber security professionals globally.

We also launched the NUS-Singtel Cyber Security R&D Lab last year to conduct research on next-generation cyber security technologies, a facility that will no doubt be cultivating and attracting top security talent to Singapore.