Publication: Enterprise Innovation
Date: 2 December 2014
Headline: University Challenge I: CIO talks modernisation at SMU

University Challenge I: CIO talks modernisation at SMU

PUBLISHED ON DECEMBER 2, 2014
BY RAHUL JOSHI

Caption: SMU CIO Lau Kai Cheong

Singapore Management University (SMU) - its campus comprising six buildings located in the heart of Singapore's city center - is known for its modern approach to education.

Emphasizing interactive, seminar-style classes and what it calls "technologically enabled pedagogy", SMU prepares its 8,300 students to be entrepreneurial leaders in a knowledge-based economy. In doing so, it strives to provide students with state-of-the-art facilities, integrating technology seamlessly into the student experience.

Doing so is no easy task. From ensuring secure Wi-Fi access throughout the campus, to providing relevant teaching and learning applications, SMU's IT team has had to grapple with a host of IT challenges. Enterprise Innovation speaks to Lau Kai Cheong, SMU's Chief Information Officer, to discover how SMU facilitates the use of technology throughout its large, sprawling city campus.

Could you talk about the IT team's role in SMU?

Our role encompasses supporting the university in terms of its core business, which is basically teaching, learning, as well as research. To do this, you also need a very strong administrative component – that's another very big area. The IT team supports the university in enabling the computing power and the facilities for research. So basically, these three areas – teaching and learning, research, and supporting effective administration.

Could you give a brief overview of the sort of computing resources you have at SMU?

I'd like to start with the network, because in any organization, not just in higher education, the network is always the most basic and fundamental part of any IT infrastructure. A strong, robust, reliable, scalable network is core to any organization, including SMU.

In SMU, because we are a very open campus, and our students are very mobile, our strategy has been to go wireless as much as possible, from day one. Because of that, we need a very secure and robust wireless network.

We revamped our wireless network about 3 or 4 years ago, because one of the challenges we faced was capacity. In the legacy network, we were restricted to a limited number of access points that could be installed on campus. And that meant we could attain only about 60-70% coverage.

We have six buildings at the moment, with a new Law School building coming up in 2017. Students are free to move within these six buildings and we want to make sure that when they move from building to building, or even across the streets, the wireless connection stays connected. Previously, we had dropped connections or weak signals. Also, feedback from faculty members showed that the signals in their faculty rooms were quite weak, since the older technology was not able to cover the whole floor.

And now, with mobile devices, everybody relies on wireless. That compounds the capacity issue, because students today, as you know, carry multiple mobile devices. They're Gen-Mobile students. And we need to make sure that the density of that wireless device, wireless component and access point are able to support a lot of students gathering at the same area, for instance, at the library. We have to boost the signals in such places.

Another big challenge I want to also highlight is security. It's a big concern for us, especially since SMU is a city campus. We are porous and our buildings are connected by an underground, public concourse. In the middle is the Bras Basah MRT station. And three years down the road, the Downtown Line is going to open and it'll be just next to our city campus. With that, it means that our network is open to the public.

How do you solve these issues?

Security is something we take very seriously and we have implemented layers of protection. But not in a way that creates inconvenience for students. The older technology access point used WEP encryption and didn't have a lot of protection. Now we're on WPA2 and we've also added a layer of protection by using a robust ClearPass management system solution. That allows us to authenticate users and apply network policies to devices attempting to connect to our network. And we also make sure that these devices comply to a baseline set of network policies before they're allowed to connect. We call this end-point security.

So all-in-all, we want to make sure that our network stays secure because we do not want any unintended attacks on our system.

Also, SMU has always been known to pioneer the use of very participative, interactive pedagogy. Class discussions take place online all the time - online discussions, online quizzes, even online exams. This, as you can imagine, relies heavily on our wireless infrastructure. We need to ensure that students have access to the wireless network all the time, especially in study areas. To this end, we often have to measure the signal strength in various areas. We also need to ensure students' work submitted via the wireless network, such as their assignments or online exams, is secure.

Publication: Enterprise Innovation
Date: 2 December 2014
Headline: University Challenge I: CIO talks modernisation at SMU

How large is your internal IT team?

The network team is very lean, only three network engineers and one manager. And because of that, we need a system that is very easy to manage at the backend. In the old technology, the APs were fat APs which contained all the intelligence configuration. This made management a lot more challenging. But now, with thin APs, the intelligence management is all at the controllers, which means there is less need to have a bigger team to manage so many APs. So that’s how we use technology to make our management a lot more efficient and effective.