

EDITOR'S VIEWPOINT

Have China take-privates spiralled out of control?

Page 4

NEWS

Affinity, Baring Asia, BlackRock, CDIB, CVC, DCM, IFC, IL&FS, JBIC, Lenovo, Mayfield, NewQuest, Samara, Sequoia, SBCVC, Temasek

Page 5

DEAL OF THE WEEK

Hotung, CDIB lead round for Taiwan-based ACT

Page 12

QIC eyes Asian demand for Australian beef

Page 13

INDUSTRY Q&A

Piau-Voon Wang, co-CIO of China's Noah Holdings

Page 15

Margins for success

India's NBFCs deliver returns by going beyond banks' comfort zones Page 7

FOCUS



Holes in cyberspace

Asia plays catch-up on high-tech security Page 11

DEAL OF THE WEEK



A cut above the rest

Farfetch brings boutique fashion online Page 12

29TH ANNUAL



PRIVATE EQUITY & VENTURE FORUM 15-17 November 2016
Four Seasons Hotel
Hong Kong



REGISTRATION NOW OPEN!

Book by 27 May and SAVE US\$1,100

Brochure available, download now at avcjforum.com



The 29th Annual AVCJ Private Equity & Venture Forum

The AVCJ Forum brings together over 1,000 of the world's leading GPs, LPs and other professionals for three days of quality discussions, speeches and networking. These perspectives come to life at the **AVCJ Private Equity & Venture Forum**, scheduled for **November 15-17 in Hong Kong**.

15 Tuesday
November 2016

PE LEADERS' SUMMIT
VENTURE CAPITAL SUMMIT
LIMITED PARTNERS' SUMMIT

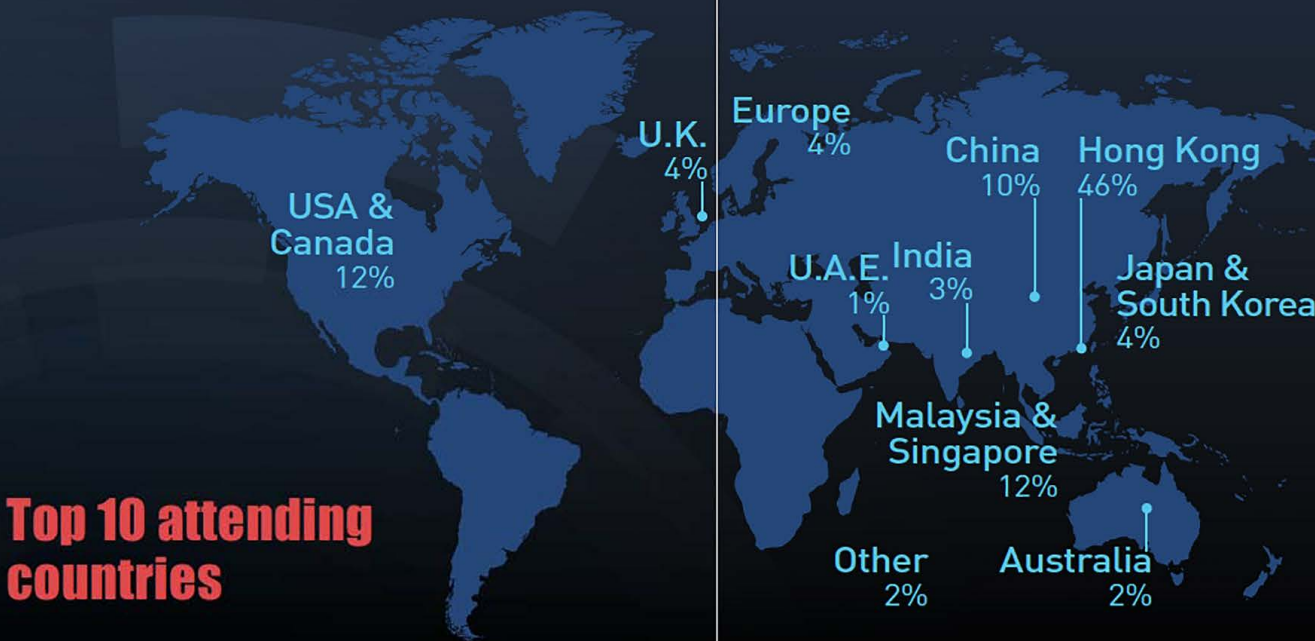
For more information visit avcjforum.com

16 Wednesday
November 2016

INVESTMENT SUMMIT (DAY I)

17 Thursday
November 2016

INVESTMENT SUMMIT (DAY II)



Top 10 attending countries

MERGERMARKET GROUP

avcjforum.com

Join your peers



Security in numbers

An unbalanced global cybersecurity market – currently weighted heavily toward the US – is slowly finding its feet in Asia. But opportunities in the expected boom may not be intuitive to newcomers

WHEN IT COMES TO IDENTIFYING

emerging investment segments that have long-term credibility, there are few indicators as convincing as the opening of a dedicated, sector-focused school. This scenario is unfolding in Singapore where telecommunications giant Singtel has unveiled plans for a 10,000-square-foot cybersecurity training facility. The Cyber Security Institute (CSI), said to be the first of its kind in Asia Pacific, follows a \$120 million government commitment to info-communications training with an emphasis on cybersecurity.

“Based on our engagements with companies in Singapore, more than 85% do not have robust cyber response plans nor the opportunity to conduct realistic drills to test and sharpen such plans,” says Bill Chang, CEO of group enterprise at Singtel. “This lack of cyber preparedness is worsened by the severe global shortfall of trained cybersecurity experts, which Forbes puts at around one million in 2016.”

This sense of urgency is supported by a Market & Markets forecast that cybersecurity spending will reach up to \$170 billion in 2020, while Lloyd’s of London estimates that cybercrime is currently costing corporations as much as \$400 billion a year. For venture capitalists, however, these trends entail a severe bias toward the US, where more than 80% of dollar funding for private cybersecurity start-ups is invested, according to CB Insights.

Singapore’s latest push to embrace the sector, though advanced by Asian standards, must therefore be considered part of a relatively late response to a global, US-led groundswell of investment support. As CSI fuels a wave of cybersecurity start-ups in Asia Pacific, VCs hoping to identify viable targets must recognize the pitfalls among the possibilities and a new range of diligence parameters.

Hot or not?

VC cybersecurity investment strategies will focus on familiar variables related to management pedigree, competitive landscape and total addressable market. But for uninitiated investors, the sector’s unique technical adaption and customer engagement value propositions are complicating factors.

“Where I see mistakes amongst investors are

angels making relatively small investments into cybersecurity because ‘cyber is hot’, says Steven Morgan, founder and CEO of Cybersecurity Ventures, a market intelligence researcher focused on start-ups and emerging companies in the sector. “The investor knows cyber is a big growing market and they want in, so they fund the very smallest ventures which carry the greatest risk and tend to have first-time entrepreneurs going to market.”

Notable Asian success stories in this space have included Trend Micro, FFRI, i-Sprint Innovations, Ahnlab and Qihoo 360 Technology, which is currently subject to a \$9.3 billion take-private bid. The region remains at a disadvantage

“The higher walls you build, the higher ladders the bad actors will bring in”

– Sanjay Aurora

at the early-stage level, however, due to a lack of an established ecosystem. This points to cross-border relations as a potential hallmark of more prospective cybersecurity start-ups.

“There are some Asia Pacific companies that have set up a US office in Silicon Valley specifically to be near VCs, which dramatically increases their chances of funding - simply because they are local and will be able to have many more meetings and speed along the process,” adds Morgan.

A recent \$12 million Series B investment for US-India firm Seclore helps illustrate the advantages of a Silicon Valley-connected profile when combined with Asian growth potential – especially in the intense data traffic context of India’s outsourcing market. Investors in the round included VentureEast, Sistema Asia Fund Advisors and Helion Resources, which cited the importance of an established customer base in a field where product validation through technical due diligence can be difficult.

India Alternatives also participated in the Seclore deal and noted key differentiators in the cybersecurity space, including a company’s ability to engage clients without complex

technical jargon and a product offering that solves a specific problem in a unique manner.

“You have to look at what specific aspect of the overall space is hard to crack, and it is security in a collaborative environment,” says Shivani Bhasin Sachdeva, managing director and CEO at India Alternatives. “Data proliferation is occurring like never before and document sharing in an external environment is growing at a scorching pace across all different kinds of devices. A lot of security solutions just provide a firewall or require implementation by the end user, which increases vulnerability to data theft.”

Outside the box

Ambitions beyond the firewall represent the innovative bent that drives tech-related fields such as cybersecurity. But at this stage, the traditional approach of building a two-dimensional defense around company data still dominates cybersecurity discussions despite the promising path forward suggested by more nuanced, customer-specific systems.

“Most resources, technology and people are still focused on saving the perimeter, whereas actually the battle is really inside the network,” says Sanjay Aurora, managing director of the Asia Pacific division for cybersecurity technology provider Darktrace. “The speed at which attacks are happening and the speed at which things are moving, it is just not possible to keep up to date with rules and signatures. The higher walls you build, the higher ladders the bad actors will bring in.”

This perspective is perhaps the bedrock of cybersecurity’s long-term appeal to venture capital. But although the endless arms race between companies and criminal hackers will invite tech start-ups to develop innovate new products, the marketability of the space remains mostly in the domain of insuring against human error and the natural challenges of managing bigger, more heavily circulated datasets.

“Cybercrime makes an interesting story, but the bigger push that we’re excited about is that businesses will continue to work in a collaborative environment and therefore the need for security in that environment is here to stay,” adds India Alternatives’ Sachdeva. “If there’s one thing we’re betting on, it’s the fact that businesses will continue to collaborate.”