RSA Conference 2019

BETTER.

Peer2Peer

Cyber-Innovation: How Do We Stimulate Innovation in the US, Europe and Asia

P2P2-R11: Cyber-Innovation: How Do We Stimulate Innovation in the US, Europe and Asia

Grace Cassy, Co-Founder, CyLon

Cyber-Innovation: How Do We Stimulate Innovation in the US, Europe and Asia

It's a truism that cyber threats evolve quickly, and defenders have to move just as fast to counter them. With over 500 vendors exhibiting at RSAC Conference 2019, you'd be forgiven for thinking that we are not short of new cyber defence solutions. But how can we keep this innovation pipeline flowing globally with the right products to tackle evolving problems?

An international group of startup founders, investors, corporates and government representatives gathered at the RSAC 2019 for a P2P Session discussing how to stimulate innovation, how to distinguish signal from noise in a crowded product marketplace and what opportunities and challenges await innovators in different regions.

We looked first at the success factors for a security startup. A consistent marker was proven sales ability. We all love technical founders, but an early team also has to be able to sell. Linked to this was having a clear differentiator in the market and an understanding of their customer's real problems. Participants felt that too many young companies hadn't asked the question "Who is buying and why?" and found themselves with a solution in search of a problem. And if a company has international ambitions, they need a diverse team with breadth of background and experience who can navigate a range of markets.

Government participants were interested to understand if there were any under-served product areas where they might target support. Our conclusion was that while most sectors are crowded, there were several where likely category winners hadn't yet emerged or where there was much still to play for: identity, IOT security and solutions to inform cyber insurance stood out.

Once a company had established itself in its home market, what regional differences should it take into account as it grows? Discussion focussed initially on regulatory regimes. A number of Asian countries were refreshing their disclosure regimes. Singapore, for example, had recently announced a new mandatory data breach notification regime, which participants felt would stimulate a new focus on security in the region, providing an opportunity for innovators. In a similar way, the advent of GDPR had stimulated creation and adoption of a new range of privacy and compliance solutions.

There were also obvious regional differences in terms of:

1. **Access to smart security-focused capital.** The US remains clearly in the lead, with Europe accounting for around a quarter of VC deals in security last year. Interest is certainly increasing in Asia, but there is currently less capital focused on security, and less familiarity with the space among VCs. Overall, though, the group didn't believe that innovation was stifled by lack of capital: good teams with good ideas will always get funded.

2. **Availability and cost of security talent.** Security skilled professionals can command high and growing salaries. Some participants felt that Europe and Asia had an advantage in having talent available at more competitive rates, while others thought mobility generally smoothed this out.

As we looked at keeping the pipeline of innovation flowing, we compared support models that participants had experienced in different regions. The Indian representatives in the room highlighted the benefit of government partnering with academia to stimulate startups, while the investors expressed some skepticism that such programmes produced truly scalable businesses. There was, however, broad agreement that government had a vitally important role to play as an early adopter of innovative solutions. Such support acted to credentialise a young company as it then sought to address Enterprise clients.

Finally, the pre-event survey had highlighted participants' concerns around skills, and we finished up with some discussion on how to encourage technically-talented people to consider a career in security entrepreneurship, against the lure of very large salary packages elsewhere. The final word on this, from a start-up CTO in the room, could be summarised as: "I do this because it's more interesting. I get to work directly on solving problems and have more influence day-to-day". Encouraging words, reflecting a really positive feeling in the session around emerging innovations.

Interested to look at other resources on this subject?

- CyLon Insights: Our Lessons from 1000 Cyber Startups
- Access to security-focussed capital: SCV summary of Cyber VC Investment
- Straits Times piece on the new Singapore data breach notification rules
- On availability of global cyber talent: Capgemini report