Security practitioners see security evolving into a business concern

By Winston Thomas

Hacks, data breaches, information misplacement and cyber espionage are grabbing headlines. Is the information security industry failing its clients, or are our infrastructures inherently flawed?

The answer is neither. Instead, the issues lie in the increasingly sophisticated and connected world we live in. And according to security experts who joined a recent NetworkWorld Asia roundtable discussion hosted by i-Sprint Innovations, the security industry itself is evolving fast to meet changing needs.

Regulations, cloud drive security

A topic of intense discussion at the roundtable was the roles cloud and regulations play in defining security's future.

"[Security] is so diversified," said Kenneth Lam, group IT director, Emperor Group. "Some industries have high security and are highly regulated, and some, like entertainment that we are part of, is less regulated. Our strategy is to go to the cloud and become mobile as I want to save my people from doing tedious work. However, this has made me focus on security in the cloud."

For Dennis Lee, executive director, head of IT Governance and Control, Asia Pacific and IT Risk Management at Nomura International, his concerns are regulations and compliance. "The main challenge in the coming year is definitely the scrutiny from regulators. It is not about tools or solutions, but rather how you want to shape your organization to tackle governance since we have more online purchases. This makes data leakage a big issue for us."

Micky Lo, managing director, head of Information Risk Management APAC at The Bank of New York Mellon, agreed. "It is not so much regulators being strict or prudent but more the inconsistent expectations. A good example is when cloud [is permitted for use] in the US but not in Asia. That causes a lot of frustration to us in terms of global inconsistency."

"We've got 11 countries," said Kelvin Lam, associate director of Strategy and Planning, Asia Information Risk Management, at Manulife (International) Limited. "We have different regulations. This makes it a huge challenge for us in Asia." Lam also noted that regulators increasingly want the data to be kept within their own borders.

Victor Cheng, executive director of Hong Kong Education City Limited, faces a different scenario. "For education in general, the concern is protecting the students' data. So, you need a system that is easy to use but also strong enough to block others who want to exploit the system." Cheng added that it has been difficult to convince conservative-minded schools to move to the cloud although a scalable and highly secure cloud service may give them the confidence to migrate.

Relationships matter

Dale Johnstone, senior system manager of Information Security and Risk Management at Hong Kong Hospital Authority, believes the future lies in Identity Relationship Management (IRM), not Information Access Management (IAM). "The two key issues that interest me at this moment is mov-

ing IAM to IRM, and the exploding potential of moving from IP-enabled devices to Internet of Everything and its impact on the healthcare environment," he said.

Johnstone explained that access management was simple in the mainframe days. "One identity for accessing whatever. But today, I may have 20 identities within the organization, and I may have 200 identities external to the organization," he said. That's why the chance of cracking a user's internal password is high because it could likely be identical to the external password.

He also noted that many security solutions rely on a siloed approach. "Single sign on and such do not tell you what you have access to. So, [IRM] is more of a business perspective. It is still a fairly new concept, but it is a difficult space."

The importance of concepts like IRM really stands out where organizations work closely with external parties. "Governments usually have external parties to manage," said Chan. "That to me is a big security loophole because you never know when they will take the easy route to manage security."

It's a concern that Lo shares. "Like most banks, we outsource," he said. "Service provider risk is a concern. We have issued new guidelines on the way we manage or provide governance over our services providers. We don't know what we don't know. That's what happened in my previous bank where we searched on Google ... and found a lot of client reports in the public domain. We traced them and found that it was a corporate marketing manager who was working at home and started doing uploads."

Biometrics no panacea

Albert Ching, CEO of i-Sprint Innovations, noted that regulators are now considering biometrics to authenticate users. "Password is not strong enough for authentication. That is why we see a lot of needs coming from regulators in terms of biometrics. In Japan, users are already using their palm [print for authentication] at ATMs."

Lo noted that JP Morgan tried using fingerprint biometrics 15 years ago. "Then, we had a push back. First was cost, especially 15 years ago, and second was people's concern around what the fingerprints will be used for."

For Johnstone, biometrics is a natural evolution – not the ultimate answer – for security. He forecast that biometrics would go the way that passwords have. "If biometrics becomes as common as passwords, they will become useless because everyone is going to have a copy of my fingerprint," he said. "I do not think biometrics is the panacea. They are good today, and like anything in security, they will, in time, get worn down. Then you have to look for something else."

On the other hand, Ching believes that biometrics technology has become more sophisticated as well.

People part of the equation

Yet, managing people is more important than the actual security solution itself. "My biggest problem is to deploy a solution. In an organization where you have everything very embedded and lots of politics, any change to any solution, regardless of what it is, will potentially involve backend process flow change," noted Johnstone. "This is very difficult. You may have the best product but the disruption to the organization may be too great, and that is another risk."

Manulife's Lam noted that access management is difficult especially when a person has gone through the ranks and acquired multiple access privileges. "There are cases where a person who had moved through different departments may acquire more access [privileges] than the CEO."

This is the reason Johnstone pays more attention to the people side of any solution. "One of the things I learnt after being in IT for so long is that in the past, a lot of people in IT were trained in business, and came through the ranks in the business. Today, a lot of them come straight out of university. They do not have front-end practical experience, and that is a bit of a challenge."

Mergers and acquisitions also complicate the management and deployment process.

Ching noted that i-Sprint Innovations has new solutions that consider geo-locations and geo-defense.

"We have products that look at [users'] current roles and map them out to the applications that they need to access," he said, adding that these solutions can help organizations to efficiently find out whether a person is misusing an access privilege.

Balancing security, convenience

Sometimes, security can be a trade-off between protection and convenience. "Students tend to be more concerned about convenience than security," said Dr Jason Chan, head of IT at The Hong Kong Polytechnic University. "If they can manage everything on their mobile, they will be very happy."

Chan once proposed to the Education Bureau a platform that uses federated authentication to control students' access to online resources. "Previously, this platform could not happen because no one wanted to bear the responsibility to hold all the student data. I suggested using the federated authentication mechanism so that the platform itself does not need to hold the student data. Now, the proposal is submitted and under consideration."

HK Education City's Victor Cheng has also started on this journey. "All the student databases have been consolidated. The different provider platforms will be interconnected as well. This offers a really unified identity management infrastructure for education," he said.

Education is vital

Nomura's Lee noted the importance of end-user education. "The problem is that some users do not know that iCloud or Google Docs synchronizes their files."

Hence, users should also be aware of the risks when connecting their devices to the company system.

To this end, Kelvin Har, CIO of the Securities & Futures Commission, observed that his role has increasingly become that of an advisor on the setting up of security policies.

"Our focus in the last two years has been on the people side," Har said. "We trying to raise awareness in the internal environment to prevent information leakage. As long they are aware, we can share our guidelines."

Beyond the cost center

For many years, security has always been perceived as a cost center. That view could be gradually changing.

"In the last four to eight months, some companies have begun using their security infrastructure as a strength to attract business, increase productivity and improve profits," said Simon Leung, chairman of i-Sprint Innovations. "And I think this is interesting. If you play defense all the time, you will eventually lose the game. Instead, you [should] attack, especially when you have a good system."

"Our clients are really other banks," said BNY Mellon's Lo. "When they contract with us to do banking services, they want us to submit our security portfolio. So, we have been promoting and using our security strengths to sell to our customers and [expand further into], for instance, corporate mobile payments."

Leung also noted that a good security system is a great source for big data. "With big data, you can go back to the business unit and tell them you know what customers are doing." In a sense, security can become a profit center, and provide new business opportunities.

But benefits can be indirect, especially in the banking sector. "Banks' main concerns are first money and second, who borrows their money," said Har. "So, generating profits may not be so direct for security, but internal costs can definitely be reduced."

Productivity can be improved as well when, for example, pre-authentication reduces online access time from 15 minutes to just one. NWA

Participants:

Dale Johnstone, senior system manager (IT Security & Risk Management), **Hong Kong Hospital Authority**
Kenneth Lam, group IT director, **Emperor Group**
Andrew Ip, chief auditor and general manager, **Octopus Cards Limited**
Dennis Lee, executive director, head of IT Governance and Control, Asia Pacific, **Nomura International (Hong Kong) Limited**
Kelvin Lam, associate director, Asia Information Risk Management, Regional Information Technology, **Manulife (International) Limited**
Victor Cheng, executive director, **Hong Kong Education City Limited**
Micky Lo, managing director, head of Information Risk Management APAC, **The Bank of New York Mellon**
Dr Jason Chan, head of IT, **The Hong Kong Polytechnic University**
Kelvin Har, CIO, **Hong Kong Securities & Futures Commission**

Hosts:

Albert Ching, CEO and CTO, **i-Sprint Innovations**
Simon Leung, chairman, **i-Sprint Innovations**

Moderator:

Victor Ng, S E Asia bureau chief, **Questex Asia**