Securing data in an SaaS world

By Cat Yong

End-to-end authentication provider i-Sprint Innovations may have had its roots in the financial services and insurance sector, but their solutions are also relevant in other industries. This is especially so now, because more and more businesses are leveraging online transactions, mobile commerce and also cloud computing services.

A PwC survey discovered that of the 1,330 companies they surveyed from 79 countries, 39% of financial services were hit by cybercrime, compared to 17% from other industries. These numbers are only going to increase, overall, regardless of which industry is in question.

Cybercriminals are also getting more active on the mobile platform, and recently, the bug called Heartbleed targeted the Android mobile platform, because users have become so dependent on their mobile devices, to the point that they would store their personal and sensitive information on them.

Questex Asia's South-East Asia bureau chief Victor Ng described trends like BYOD, enterprise mobility, social media and the cloud as becoming more pervasive, but with the shadow of a very strong and sophisticated cyber underworld looming in the background -- while our world gets more hyperconnected as we move into the "Internet of Everything".

"The trouble is we can't live without technology," he said. "To some extent, when it comes to customer convenience, technology is winning the war.

"With the trends being so, we have to be ahead before the threats catch up and overtake us. To make convenience for customers really effective, we need to mitigate the risks with some form of privacy and security."

With this in mind, NetworkWorld Asia's recent breakfast roundtable host-

ed by i-Sprint Innovation tried to find out from IT heads their views on how best to improve convenience for end users and customers while protecting their data and privacy.

"Does your organization's approach to providing customers the convenience they need, also able to meet the increasing need for security and privacy?" Ng asked.

Technology and security: the necessary evils

The cloud computing industry had more than tripled in size from USD46 billion to USD150 billion, between 2008 and 2014. Today, it is also common to have 10 or more software-as-a-service (SaaS) applications used across an organization and within departments.

This number will continue to grow, and as businesses and their users' expectations increase, the challenges that come with the prevalence of SaaS become more complicated. How do businesses leverage the convenience that technologies like mobility and the Internet offer, without putting themselves at risk, from a security as well as from a compliance perspective?

Security that is too stringent, with long arduous passwords and many of them to remember and occasionally change, can be a productivity inhibitor, for example.

Dr Sukdershan Singh, deputy director at the Ministry of Health's Telehealth Division opined: "A solution according to ISO standards, may be the best, and ticks all the boxes. But when it comes to user-friendliness, it's another matter altogether."

How then do businesses implement a security solution, so that it is allowed to work for the business, without getting in the way?

Bank Simpanan Nasional's senior vice president and head of Transformation Management Department, Alain Boey, summed it up: "There are real security concerns here, because online banking is still one of the key channels for banking transactions."

As customers and business users demand more services and higher quality of experience, mobility is fast becoming another channel for banks and businesses to do transactions.

Boey said: "As we go into mobility, how do we secure all these mobile transactions from customer sites?" Essentially, this boils down to also enabling trust when users can't see the person on the other end of the mobile, online or phone transaction.

Reputation and financial protection

Security isn't only about protection against financial loss. It also has to take into consideration personal privacy and reputation. Dr. Singh painted a scenario of celebrities, VIPs or persons of interest, being admitted to hospitals or clinics. How do they keep their personal patient information away from the prying eyes of hospital staff?

i-Sprint CEO and CTO Albert Ching rightly observed that "it is not about money anymore, but about reputation. If there is no trust in the system, [technology] will not work."

For example, the convenience that technologies like cloud computing offer, can't be realized if they are not secured, or if there is no way to authenticate data with its owners.

The Malaysian Health Ministry is currently implementing the Health Information Exchange (MyHIX) project, which aims to connect all 142 hospitals and the more than 1,000 clinics in the country to enable secure and convenient exchange of medical records among these hospitals and clinics.

The end goal is for Malaysians to be able to walk into any MyHIX networked hospital or clinic and have their medical history readily accessible for the attending physician's reference. This is supposed to work in tandem with Malaysia's national identification card or MyKad, that contains a smart biometric chip with the patient's credentials.

Ching said: "You need to have a certain trust level before you can share patient data. How do users or patients securely authenticate that the data in the system belongs to them?"

Pacific Insurance's senior manager of ICT and Research, Rohana binte Ismail, also recognized the benefits of technology, and how it can actually be leveraged to automate processes and cut down redundancy and paperwork.

But for any third-party entity like an insurance company, to have access and be linked to a database of health concerns or the Road Transport Department database, for example, raises potential issues of privacy and fraud – it may open the whole system or database up to the risk of compromise or theft.

Further, data owners should be the ones to decide who has access to their personal information, especially pertaining to matters of health.

Tech challenge and opportunity

There was consensus around the table that Malaysians find it difficult to really take advantage of certain trends like BYOD, when there is poor quality of mobile connectivity in the first place.

Berjaya Group's senior general manager and head of Group IT Eugene Chung said: "A lot of solutions look good on paper, but are difficult to deploy especially when there are challenges with the mobile connectivity."

How does a business realize the benefits of end-to-end data encryption, for example, if poor bandwidth is going to dampen the experience of the employee on-the-road?

There was also consensus that internal threats are cause for concern, just as much, if not more than, external threats.

Here, i-Sprint's director of Product Management and Solutions, Priyesh Panchmatia, shared how security technologies like facial recognition with ID tags could be used in tandem, to protect desktops from prying eyes in the workplace, as well as to increase productivity.

Ching added: "We do see a convergence of security technologies like biometrics, physical tags and location awareness. And these are being used in many industries currently." He also observed more active usage of RFID technologies in the future.

Conclusion

According to Ching, industry input is important for vendors to validate their research and development focus and their solutions roadmap.

He believes security is a process, which looks at the human aspect, the environmental aspect and the technological aspect, as well as compliance if the industry is regulated, to ensure the security solution fulfills business expectations.

Ching opined that the dreaded possibility of vendor lock-in can be overcome if standards are set. He recommended a system based on standards that allow other solutions to be plugged in, addressing scalability and future-proofing at same time.

"A supposedly 'open' system could still lock you in, if you don't design the implementation according to standards," he said.

Hence, technology is just a tool, meant to be deployed based upon the unique requirements of the business and what it wants to achieve.

And when one studies the challenges that each industry faces, it all boils down to a few fundamentals that every business wants to achieve – security and privacy with access, convenience and productivity. NWA

Participants:

Chua Sze Hun, regional head of Information Security, **Eastspring Investments Limited**
Eugene Chung, senior general manager and head of Group IT, **Berjaya Corporation**
Ms Rohana Ismail, senior head of ICT and Applications, **The Pacific Insurance Berhad**
Alain Boey, SVP of IT and head of Transformation Management, **Bank Simpanan Nasional**
Dr Dang Siew Bing, deputy director, IT, Ministry Of Health, Telehealth Division, **Operational Unit**
Dr Sukdershan Singh, deputy director, IT, Ministry Of Health, Telehealth Division, **BPR/CM Unit**

Hosts:

Albert Ching, CEO and CTO, **i-Sprint Innovations**
Priyesh Panchmatia, director of product management and solutions, **i-Sprint Innovations**

Moderator:

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