An Enterprise Innovation Guide

Cloud Security

Cloud security not just an IT question

Published by QUESTEX MEDIA Enterprise INNOVATION

Sponsored by hp

Security. It's more important than ever.

Get the right security for wherever your workforce is taking care of business. Manage risk with comprehensive HP solutions that work across your organization and around the world.

hp-enterprisesolutions.com

Table of Contents

Enterprise INNOVATION

Managing Director **Jonathan Bigelow** jbigelow@questexasia.com

Group Publisher **Simon Yeung** syeung@questexasia.com
Regional Account Director **Clarise Goh** cgoh@questexasia.com
Account Manager **Careshma Ramroop** cramroop@questexasia.com

Group Editor **Chee Sing Chan** cchan@questexasia.com
Deputy Editor **Rahul Joshi**
Contributing Writers **Jason Krupp, Dylan Bushell-Embling**

Art Director **Dick Wong** dwong@questexasia.com

HR & Admin Manager **Janis Lam** janislam@questexasia.com

Accounting Manager **Nancy Chung** nchung@questexasia.com

Director, Audience Development – R&D **Will Ahmad** will@questexasia.com
Assistant Circulation Manager **Shipman Kwok** skwok@questexasia.com

QUESTEX MEDIA

Editorial and publishing office
Questex Asia Ltd
13/F, 88 Hing Fat Street, Causeway Bay, Hong Kong
Tel: +852 2559 2772 Fax: +852 2559 7002
Website: www.enterpriseinnovation.net
Subscription Hotline: +852 2589 1313
Subscription Fax: +852 2559 2015
E-mail: customer_service@enterpriseinnovation.net

Cloud Security Guide is published by Questex Asia Ltd, 13/F, 88 Hing Fat Street, Causeway Bay, Hong Kong. Printed in Hong Kong.

Public and private cloud to increase by 50% by 2020

ALMOST 70% OF business and technology executives in APAC believe that cloud computing will be at least as disruptive to the technology landscape as the impact of virtualization or the internet, according to Coleman Parkes Research's survey findings. Commissioned by HP, Coleman Parkes' survey, titled: The Future of Cloud, revealed that senior business and technology executives expect public and private cloud delivery models to increase by 50%.

The other key findings of the study include: Currently, only 27% of enterprise delivery models are cloud-based. The top three barriers to cloud services adoption are security concerns (35%), transformation concerns (31%), and compliance or governance concerns (16%). Business and IT executives recognize that cloud implementation will be critical to driving successful outcomes and innovation. About one in two CEOs and CFOs are currently setting cloud strategies for their organizations.

Murky forecast still projected for cloud security

DESPITE THE BEST efforts of cloud service providers and industry groups, cloud security remains a troublesome issue for IT execs. At an RSA session earlier this year devoted to cloud security, IT security pros complained about the lack of transparency among cloud providers and how that makes it extremely difficult to make informed buying decisions.

Attendees in the audience pointed out that there's currently no certification for cloud security. So, where does that leave IT execs? Nils Pulhman, former CSO at Zynga, suggested that IT execs grill prospective cloud service providers. In his experience, particularly with startups, "nine out of 10 fall apart" when you ask the tough questions.

Cloud to capture 10% of security market by 2015

CLOUD COMPUTING IS transforming the enterprise IT security market. Gartner expects 10% of IT enterprise security products to be delivered via the cloud by 2015. The research firm predicts that the cloud-based security services market will surge to US$4.2 billion by 2016.

Cloud-based security services are having a particular impact on buying behaviors in segments including secure email and web gateways, remote vulnerability assessment and IdentiCloud boosting profits, helping start-ups start

A majority (56%) of cloud computing adopters believe the technology has helped them improve profits, while nearly nine in 10 report it has helped them save costs. These are among the key the findings of a survey by the University of Manchester's Business School, commissioned by Rackspace.

Start-ups are also gaining from cloud computing, the survey suggests. More than 90% of companies polled which had been established in the last three years agreed that the infrastructure savings offered by cloud computing had helped them get their business off the ground.

Cloud computing model requires security rethink

Transformation of IT operating models brings disruption to security frameworks

By Enterprise Innovation editors

Lawrence Ong at HP: Cloud security is more than just physical controls

CLOUD COMPUTING and other technology mega-trends are transforming modern IT today. Technology is being integrated into every facet of the business, and IT is rapidly transforming into a business enabler.

As cloud computing gives users access to new scale, new capability and flexibility, IT departments are likewise being required to rethink their approaches to security, while retaining the core principles on keeping companies and their confidential data secure.

Lawrence Ong, general manager for Enterprise Security Services at HP Enterprise Services, Asia Pacific & Japan, noted that "security is always a top concern for cloud adoption."

Security to risk management

Due to the changing face of IT, Ong believes that the traditional approach to security – with its focus on the hardware and software – is old-hat. "We need to move from security into what we refer to as risk management," he said.

"At HP we describe security as having three key Ps, people, processes and products or technology. You may have the best technology but if your employee goes around sticking post-it notes on their monitors with their username and password, no amount of best technology can help you overcome that violation."

Part of the issue with focusing on the technology is that it means security discussions are often phrased in the way business leaders might not understand.

"Talk to business owners about firewalls, NTFS or antivirus and you will find that the care factor is not that great," Ong said. "The language security professionals use is not aligned to the business language, and so to avoid misconceptions and misunderstandings it is essential that we keep our messages simple and avoid security acronyms and jargon."

At the moment IT risk management is very much the scope and remit of CIOs and CSOs, but as IT becomes more of a business process enabler, it will become an enterprise-wide issue. "Then we'll eventually move to what we call enterprise risk management," Ong said.

The risk discussion

Companies adopting cloud computing need to identify which assets, whether information or systems, support the most critical business processes within an organization.

> The language security professionals use is not aligned to the business language of today

Once this is complete, companies need to ask some simple questions, Ong said. "In the event that this system becomes unavailable, what is the impact on your business? If the information gets lost, does it cause your company major problems such as financial loss, exposure to litigation, loss of client or citizen confidence, or loss of brand image?"

This approach frames security and risk in clear terms that the business can understand and act on.

Key challenges

But one key assumption of the new risk management approach to security is that while it may be possible to minimize risks, it is not always practical to eliminate them entirely.

As companies dealing with stricter regulation regarding the handling of credit card data know all too well, "at some point in time, the ability to contain the risk becomes impossible," Ong said. "So this is where the executive committee within the business needs to address and accept the risk."

Some of the risk can be offloaded through commercial contracts with cloud providers, and can even potentially be alleviated for both parties by outsourcing it to an insurance organization. But if it cannot be outsourced, then organisations may have to accept the risk of a negative business outcome.

Migrating to private or public cloud services creates a number of risk and security issues that need to be addressed.

Many of the challenges will be familiar to organizations with experience using IT outsourcing. As a general rule, Ong estimates that the procurement process will typically be 80% similar for cloud and outsourced IT services.

When moving to the public cloud, business information is no longer in the hands of the company. To preserve business confidence that this data won't fall into the wrong hands, encryption has emerged as a "key enabler," Ong said.

With a private cloud model, this is not as important, as the data is typically still on-premise. But there are security concerns that must be considered even in this case, namely VM sprawl, where virtual machines are created without being managed.

Ong said these issues can be avoided if you have formal processes around information lifecycle management, or how systems are created and de-commissioned within your organization. "It depends on the maturity of lifecycle management within your private cloud."

He said the real challenge around the cloud relates to data integrity, and the various regulatory regimes some companies are working under.

Organizations in certain heavily-regulated industries are required to be able to prove where their data is at any time, in the event that the regulator has to bring a case against that company. This poses a problem when companies are using public cloud services such as Office 365 or Google Docs, because the data processing is so heavily distributed.

"That's the challenge for business, you may have the best intent but due to the way systems are built, these cloud providers might not have that ability to meet the regulators' requirements," Ong said.

Access management

The Cloud Security Alliance has formulated a series of best practices for cloud adoption and control.

These best practices combine ISO and other standards with entrenched frameworks adopted by American companies. Ong noted that one key element common across the various standards and frameworks is a focus on access management.

Organizations' approaches to access management need to take into account that employees are going to be making use of both Software-as-a-Service (SaaS) and traditional enterprise applications, Ong said.

The best practices thus focus on how to consolidate applications for both in-house and cloud-based applications.

But the issue again becomes relaying the importance of access management to the rest of the business, Ong said. "The ability to communicate in a non-technical perspective in the language of the business owners and the marketing officers – who might not be aware of the risks – this is where the challenge is for the industry."

The security life-cycle

Cloud security is more than just physical controls. Just as important are the other two Ps in Ong's three P's of security – the policies and the people.

"What we advocate within HP is basically what we call security lifecycle management," Ong said.

When helping a client move from siloed systems to the cloud, HP starts by reviewing a company's strategy and policies, and provides recommendations on how they need to be updated.

Next the company tackles the governance and policy layers, to make sure there won't be any issues at the employee level.

Then HP helps companies introduce technologies to automate the controls, the processes and people.

This holistic approach "helps you reduce your risks, which then helps you adopt the new technologies that can support your business," Ong said.

Cloud security not just an IT question

IT leaders suggest cloud strategy must be based on assessment of business case and risk before deployment occurs

By Dylan Bushell-Embling

DUE TO IT'S promise of unprecedented business agility, most large organizations have adopted or are considering adopting some form of cloud computing.

Even the most reticent of companies will soon find the cloud seeping in around the edges, due to their employees' use of personal cloud services.

But any migration to the cloud needs to be carefully managed to ensure that business critical data remains safe. Organizations need to set clear policies around data protection, and employees need to be educated about the risks. This requires the involvement not just of IT, but of the wider business.

Cloud adoption is inevitable

IT leaders are coming around to the reality that cloud adoption is going to happen, whether they want it to or not.

Fuller Yu at AIA: Start by establishing a cloud strategy which includes a clear set of principles built around risk assessment

Richard Stagg, managing consultant for security firm in Hong Kong, Handshake Networks, noted that in practice, saying 'no' to the cloud "just doesn't work".

Stagg joined other security experts and heads of IT to discuss the challenges of cloud security at the recent InfoSecurity Conference 2013 in Hong Kong.

"If IT does say 'no' then the staff who want the service will just go out and procure it anyway. Then you end up with shadow IT, with unmanaged cloud services that are not going through the due diligence processes," Stagg added.

There are of course security challenges and risks associated with cloud, and the IT department may sometimes need to step in to veto a particular provider or steer people to a more enterprise-focused service, he said.

"But in the grand scheme of things internal IT just cannot provide the same flexibility, the capacity, and the ready-made applications that are available on the cloud. At this point, if people want to use these services, if there is a business case, then of course they must. The IT department should never be standing in the way of that."

Alex Skilton, senior manager at KPMG, agreed that IT needs to walk the fine line between enabling and being a gatekeeper. This is where a clear set of cloud principles that can be used to assess risk can be invaluable.

But this also requires IT to engage with the rest of the business on strategy discussions, he said. "Unfortunately in IT sometimes we're just masters of getting the job done rather than being able to have that strategic conversation. I think that's the main challenge."

Start with cloud strategies

As important as it may be, security is rarely the starting point for any discussion about moving to the cloud.

Fuller Yu, Head of Technology Risk, Technology Governance, Group Strategy, Technology & Operations at AIA Group Limited, said it's important for any organization to start by establishing a cloud strategy which includes a clear set of principles built around risk assessment and security.

Yu said AIA uses an underlying cloud strategy as a starting-point, then considers the business case for moving a process to the cloud. If it meets the criteria, then IT starts thinking about the data that's going to be shared. The next step is devising strategies to protect it, and developing an understanding of the risk of having the data in the cloud.

In this context, "info security is just another way to make sure we help the business to make a decision, help them to take a risk," he said.

Cloud procurement

It is also imperative to keep security principals in mind when selecting a cloud provider and penning a service contract.

The good news is many organiza-

> The personal cloud has led some security specialists to declare that DropBox is the new USB threat

Zoran Iliev: It goes back to the same issue companies have faced for years – classification of data

tions have already experienced outsourcing IT services to a third party, and most of the techniques and processes used for assessing providers and ensuring security requirements are met, still apply when choosing a cloud provider.

KPMG's Skilton said many of the third-party risk assessment concepts are the same between IT outsourcing such as Software-as-a-Service and cloud computing.

"We would recommend that the standard third-party assessment that you go through shouldn't really be changing," he said. "It's all about making sure you understand the requirements of the service [and] build those into a contract."

A subtle but important difference between the outsourcing and the cloud computing model revolves around ownership and control of a company's data. Skilton said under the SaaS model, companies arguably have less control over their data, with SaaS providers able to "pull the plug" at any time.

But for the cloud model, "the balance of accountability, of ownership of the data – the control if you like – between the provider and the customer is perhaps more [even]," he said.

Stagg agreed that the cloud model allows for more fine-grain control. "With outsourcing it's technically sort of all or nothing, whereas cloud gives you a real sort of analogue volume control over exactly how much you outsource."

But from a security perspective, some of the same challenges faced by adopting the outsourcing model also apply, Stagg said, giving examples of establishing SLAs and a right-of-audit.

Whether deploying a private cloud on virtual servers, or signing up for a public cloud service, KPMG's Skilton said it is important to hammer out agreements on how data would be managed – and who else has access – at the negotiation stage.

"Throughout the contract, [organizations should] have the right people at the table to ask the right questions, so that a provider doesn't have the ability to give some sort of vague assurance without it being solidified through a professional agreement."

Policies and the people problem

The reality that employees will adopt cloud services with or without IT's blessing puts the onus on the department to ensure that business-critical data remains protected. The rapid rise of the personal cloud has led some security specialists to declare that DropBox is the new USB threat.

Zoran Iliev, Master of eForensics and Enterprise Security and Certified Interpol TT Computer Forensics Instructor, said this this is not an entirely new problem. It goes back to the same issue companies have faced for years – classification of data.

While there are controls that can be used to detect if employees are moving classified data to places they shouldn't – using techniques including hashing and metadata – it is also important to have clear rules and policies for employees, Iliev said. "And if we have rules, we need to follow them up, we need to re-enforce them and explain them."

Stagg noted that this is a company-wide problem. "One of the things that always seems to be missing from the discussion [about] the challenges of the personal cloud...is, where are the HR guys? IT can't enforce anything, I'd like to give someone a kicking, I can only make guidelines."

HR should be working with IT to help inform employees about data policies, and periodically remind them about the rules, he said. "And when they find somebody who's been stashing things in their Dropbox, give them the previously-mentioned kicking."

This will likely become increasingly important now that the next generation are joining the workforce.

Many business leaders have expressed concerns that these workers are so accustomed to hyper-connectivity, social networking and powerful consumer devices in their lives as consumers, they may not have the expectation that they should behave differently at work. Without education, they may not intrinsically understand rules around protecting sensitive data.

"The new generation of people come to the workplace, and they do have some expectations," AIA's Yu said. "So I think it poses a challenge not only for the IT people but for the organisation themselves."

Zoran added that the problem boils down to a lack of communication. "I believe that the biggest issue is that no-one's talking about it. If we made the effort to explain [the rules] and tell them about it, I believe it will work."

Cloud, consumerization and mobile put spotlight on revising the security strategy

Every business decision has inherent risk, and it is essential to understand and make decisions based on the cost and potential value of that risk. CIOs and CISOs no longer lay awake at night worrying just about defending their organization's perimeters and the latest worm outbreak. The challenges facing security leaders today are far more complex.

Consider these recent trends and their impact on risk:

Cloud: CIOs see the benefits of cloud computing: leveraging standardized applications, reduced maintenance, pay-per-use models, and reduced capital expenditures. But risk is inherent with cloud services. Not only must CIOs maintain compliance, privacy, and transaction integrity, but they must also extend these across the service supply chain that comprises the cloud services they are using.

Consumerization: Today's employees bring personal devices to work and take work devices home. For many, there is no longer a hard line between work and home devices. This can present challenges – controlling network access, identity, application permissions, and other elements is much more difficult than ever before.

Mobility: Working at home, on an airplane, or in another city or country has become commonplace. Now data has a level of mobility never experienced before, yet laptops, tablets, phones, and even printers must accommodate secure operations.Obviously, several issues have arisen from the reliance on a traditional approach to security. Many enterprises now have a patchwork of processes and technologies that simply don't work well together. Maybe it's time to rethink security in a broader context and to bring everyone in your enterprise together – across silos and functional roles – so that you can protect what really matters: the information capital running through all your business processes.

Sustainable security ecosystem

The challenge is to create an integrated ecosystem that can not only anticipate but also prevent threats, wherever and whenever they affect your enterprise.

Think about:

- Managing risk in the era of IT consumerization mobile computing, cloud adoption, rampant cyber threats, and the spread of social media technologies
- Protecting against increasingly sophisticated threats
- Improving detection of and reaction time to security incidents
- Reducing administration costs and efficiently spending security dollars
- Achieving compliance in a predictable and cost-effective way

HP addresses the above tasks by first establishing a framework to link information security management and governance with the operations and technology required to achieve end-to-end security.

The HP Enterprise Security Solutions framework comprises three major elements:

1. Information security management
2. Security operations
3. Discrete security capabilities for data center, network, application, and endpoint security

In developing an effective strategy for enterprise security, it is important to understand that, along with the technology component, people and processes come into play as well. By combining the three elements of people, process, and technology you are able not only to build a cohesive and integrated solution, but also to mitigate compliance risks and manage compliance requirements, whether they are regulatory, commercial, or organizational. The resulting solution is fit for the purpose as well as cost-effective.

Enterprises clearly face an ever-increasing need to bring products and services to market faster and to meet the increasing demands from consumers, citizens, and

> The personal cloud has led some security specialists to declare that DropBox is the new USB threat

governments. Cloud computing promotes better ways to source, deliver, and govern highly flexible, scalable business-driven services.

Shifting mindset

This transition entails a shift of focus from technology to services. So organizations must move beyond the data center and "up the stack" to include applications and business processes to achieve greater value from their IT.

That's where the cloud and everything as a service (XaaS) come in. The cloud enables the access and use of low-cost, easy-to-use, and flexible hardware and software components via Internet technologies. Through the cloud, everything will be delivered as a service, from computing power to storage to business processes to personal interactions. Applications run the business, so there needs to be a seamlessly integrated, end-to-end view of all the infrastructure's applications, infrastructure, services, and management capabilities.

There are many technology, business-model, and sociological barriers that need to be addressed before all application domains can move to the cloud. And while that trend towards cloud gathers pace, companies will see that tremendous economic value can be unlocked when application domains reach the appropriate economies of scale.

But applications that are built from the ground up today need to be cloud-ready. Developers should take into account several security, availability, and performance considerations when adjusting or building applications for cloud.

Cloud security considerations

From a security perspective, there is a movement toward an integrated security approach as opposed to the bolt-on security implementations of the past. It leaders should look to implement standard security practices such as overwriting sensitive memory storage upon exit and ensuring that sensitive data is not packaged in Virtual Machine Images. Additional cloud security practices should include enforcing identity management and separation of roles, as well as adoption of ISO 177799, SAS 70, and PCI DSS practices.

Performance issues

In light of the cloud trend, the key components of modern application development must include: replication capability (in conjunction with the infrastructure capability), load balancing, and clustering needs. And when it comes to performance, developers need to consider the impact of network latency and bandwidth on application performance. Furthermore, the development process needs to take into account the application scalability needs and allow for performance and stress testing.

To enable a complete cloud-model transformation, there must be dynamic orchestration of custom applications, middleware, database, operating systems, and infrastructure components. There should also be a change control mechanism for workflow and governance across the lifecycle.

Focusing on "always-on" service delivery is no longer optional – it's essential. And in a hybrid delivery environment that promises greater control and flexibility, enterprises and governments should examine offerings such as cloud and services based on functionality and fit, and deploy those that deliver the desired business outcomes.

These considerations must be applied throughout the traditional IT, cloud, and even in-house solutions that an enterprise deploys. ●

Rethink security strategy with HP

HP ENTERPRISE SECURITY SOLUTIONS can help solve the risks associated with the runaway pace of security issues. Our security methodology – developed over many years of practical experience in identity, network, application, and endpoint security – helps shape the enterprise defense system in a way that supports business/government objectives.

HP secures your entire IT infrastructure by addressing all aspects of security – people, processes, technology, and content. We protect your assets and resources while helping you comply with today's regulatory environment.

The HP Enterprise Security portfolio is built on HP's rich portfolio of products and services. Our approach is to carefully align security to ever-changing business and government demands in a way that secures assets, resources, and information to manage risk and protect innovation.

Proven capabilities, proven results

HP employs more than 3,000 security and privacy professionals and holds more than 600 security patents. Worldwide, our Enterprise Security Solutions:

- Discover more than four times as many critical application vulnerabilities as other solutions in the market combined
- Prevent 550 million junk mail and 1.7 billion spam messages from reaching users monthly
- Detect and quarantine 45 million instances of malware annually
- Secure more than 1 million applications and 2 billion lines of code for clients
- Collect, store, and process 3.5 billion events daily
- Support more than 3.8 million smartcards, 1.3 million tokens, 34 certificate authorities, and 54 million usernames and passwords

Find out more

For more information about designing a layered system of defense for your enterprise, please email: ***enterprisesolutions@hp.com***

Can banks overcome their fear of cloud?

By Omid Mahboubi, Asia Cloud Computing Association

NEPHOPHOBIA is the abnormal fear of clouds, something that banks and financial services institutions relate to. Things we do not understand are usually terrifying because we just do not seem to quite figure out what they are capable of doing to us. This fear is the primary reason why organizations tend to maintain a better-safe-than-sorry attitude when it comes to cloud computing.

However, banks are generally IT-enthusiasts. Gartner predicts the banking and securities sector will spend $84 billion on IT by 2016, making this sector the biggest IT buyer of any vertical (insurance is 4th). Financial services CIOs fully appreciate the advantages that information technology has to offer. Cloud computing, however, is not like any technological disruption they have seen since the internet itself arrived, and that demands caution.

To identify the fear, a bank needs to answer the following questions:

- Are the existing cloud models mature enough to comply with regulatory regimes? Can I be properly audited? Where is my data sitting at any given time?
- What if it is not secure enough? Banking-class secure enough? Isn't cloud an open invitation to cyber criminals?
- How different is cloud from other outsourcing initiatives we are already engaged with? Should we follow the same approaches here, e.g. extensive analyses, risk assessment, SLA discussions, etc.? Simply put, how much headache are we talking about?
- Am I in control?

The answers to some of these questions are very subjective and require a thorough understanding of a bank's architecture and business processes. The result of this exercise, however, can be a step towards a rewarding cloud journey.

Analyze your cloud fear

The next step would be to analyze this fear. A history of IT outsourcing failures could well be triggering your anxiety.

Was your last IT outsourcing decision regarded as a responsibility outsourcing? Have you recently convinced your CFO to approve a budget to build a data center? Have you just recovered from a security breach? That is, have you recently fought for and implemented an IT project in your organization, and migrating to the cloud would mean you will have to admit the previous project was not a good idea?

A part of a thorough analysis is to link the cloud to your desired outcome. There are ways in which Cloud Computing can contribute to regulatory compliance or security. Think about leveraging cloud technologies to have a flexible architecture able to easily implement Basel III, for example, or how cloud is contributing to the feasibility of brand new identity management practices.

Take control

One way to break free of a fear is to confront it head-on. This is a phase where a cloud solution is deployed, making management more comfortable with the phenomenon. Choosing a financial-sector-friendly cloud service provider for a non mission-critical part of your business could contribute to the sense of control. This, however, should be seen as one stage of a broader cloud implementation roadmap.

I do not know of a financial institution or any other institution for that matter that cannot benefit from cloud computing one way or the other.

First, one needs to migrate their mind-set to the cloud before migrating their IT function.

The process starts with a change in perception, although not every C-level executive is an instant convert after the previous steps. This is time to start looking at cloud computing not as an individual technology but an IT consumption/delivery model.

Deutsche Bank Research suggests that banks in Europe spend two-thirds of their IT budget on running the bank and one-third on changing the bank. Changing how you think about cloud helps understand what roles cloud is capable of playing to potentially reverse this ratio. It would probably be a good idea to focus on evolving into a 'smarter' bank. ●

Omid Mahboubi is director of Business Development, Malaysia Chapter Director and podcast host at the Asia Cloud Computing Association

www.enterpriseinnovation.net