FSI*Review*

Deloitte Southeast Asia
Financial Services Newsletter
Issue 7, October 2014

From revolution to evolution
Gearing up for the new era

In this issue:

Deloitte.

Foreword

In this issue

There is little doubt that the financial services industry has already undergone a digital revolution. In the mobile technology arena, for instance, we have already seen a proliferation of applications as financial institutions have been relatively quick to jump on the mobile bandwagon. Banks, in particular, appeared to have achieved the greatest awareness and usage at this point in time as compared to the other industry sectors. But this is not to suggest that banking is necessarily ahead of the other sectors in terms of mobile capabilities. Indeed, even banks have not fully utilised the mobile technologies available today, such as biometric authentication, video features, and location sensing.

Perhaps what is even more troubling is how the financial services industry remains stuck in a me-too mode when it comes to technology: most innovations, if any, are slight and can be easily replicated by competitors. Should they wish to achieve a sustainable competitive or even first-mover advantage, financial institutions will need to think of technology as a key differentiator and enabler for objectives that go far beyond simply cost control or revenue generation. In other words, their digital capabilities will need to evolve.

In this issue, we explore mobile banking in a post-channel world and ways to enhance customer engagement through mobile offerings. Later on, we also take a look at some of the lessons gleaned from the front lines on cyber-risks, which will inadvertently be heightened with increased digital usage. Next, we share our perspectives on the income tax treatment of hybrid instruments in Singapore and the final version of IFRS 9 *Financial Instruments*. Finally, we present a commentary on Management Information for banks.

As the industry continues to evolve, Deloitte's Financial Services Industry group is committed to providing insights on the issues most important to financial institutions. The aim of our practice is to help guide clients through challenging times and provide the insights that are required for success.

We hope you will find our latest FSI*Review* informative.

Ho Kok Yong
Southeast Asia Leader
Financial Services Industry
Tel: +65 6216 3260
Email: kho@deloitte.com

New vision and new strategies
Mobile banking in a post-channel world

"In a world of excess and surplus, the banking industry is facing the challenge to completely rethink their customer experience and relationship model. Banks need to create key differentiators – such as high-value innovation in personal finance, as well as security and authentication – to engage their customers. However, looking forward, differentiating the mobile customer experience, thanks to analytics, is likely the most effective strategy."

Yacin Mahieddine, Executive Director, Consulting, Deloitte Southeast Asia

The full potential of mobile technology remains largely unrealised, in no small part because banks persist in viewing mobile as a separate channel rather than an across-the-board enabler. This view is reflected in the way retail banking operations are structured and how resources are allocated.

In spite of growing usage rates, many customers have yet to adopt mobile banking. Perhaps more troubling, the industry remains stuck in a me-too mode: slight innovations, quickly replicated, bring no significant advantage to the pioneer. Meanwhile, many banks have yet to go beyond cost control and drive revenues through mobile. And perhaps more importantly, banks haven't fully leveraged the mobile technologies available today, such as biometric authentication, video features, and location sensing.

The growing ubiquity of mobile devices, the proliferation of mobile endpoints, and the rapid evolution of mobile technology challenge banks to revisit old assumptions about mobile's role in customer interactions. In the not too distant future, the notion of "mobile" will evolve to include a multiplicity of devices, beyond smartphones and tablets. This will force banks to rapidly adapt to the "post-channel" world, where channel distinctions are less important and improving customer experience becomes the supreme goal, no matter where or how customer interactions occur, whether at a branch, an ATM, online, or via a mobile device.

In our view, a post-channel vision shares characteristics with the much-discussed omni-channel concept. But it goes further in visualising the degree to which mobile can fuse with branches, ATMs, and other avenues to create new and seamless customer experiences.

The basic plan is simple. Increase mobile adoption as a first step to maximise potential impact. Next, differentiate the mobile experience to boost customer loyalty. Differentiation and engagement, in turn, may enable banks to move beyond cost savings to monetisation. These steps won't complete banking's transition to the post-channel world, but they are critical foundational elements.

Fix security and perception issues to increase usage

Banks need more customers to use mobile services to explore the full potential of mobile banking. Despite increasing adoption rates, many (especially older) customers have yet to use mobile banking for even simple services, let alone more complex interactions. According to a recent survey conducted by Deloitte, a third of customers don't even use mobile to check an account balance, one of the most basic features (Figure 1).

The survey also reveals that security fears impede wider adoption. Nearly two-thirds of smartphone users are extremely or very concerned about the security of their mobile devices for banking activities, and more than 80 percent of these respondents say this worry has severely or moderately restricted use of mobile devices for financial services.

So what can banks do to overcome this concern? Educating customers to be vigilant about information protection, particularly on public Wi-Fi networks, could alleviate some security concerns. Strengthening authentication methods (via biometrics, for example) could prove even more useful.

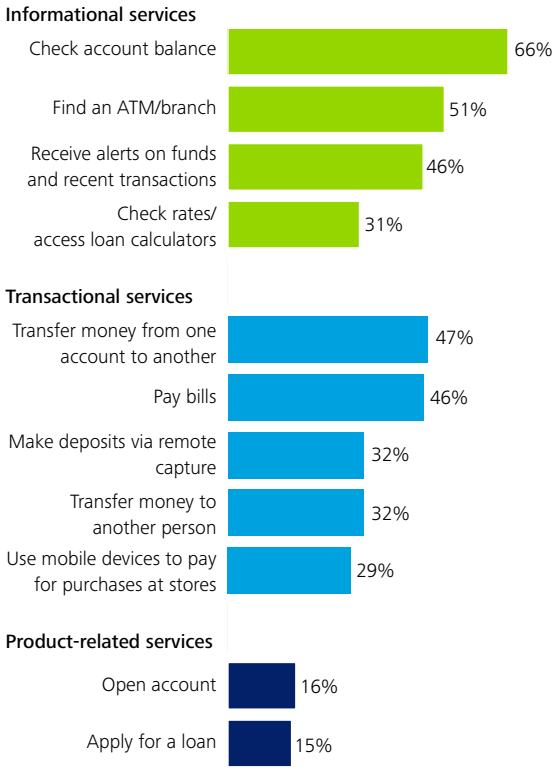
Create mobile differentiation to win loyalty

Increasing mobile adoption is only the first step. To engage and retain their growing mobile-user base, banks should differentiate their mobile offerings.

So far, this differentiation is lacking. Large banks' apps may have more advanced features than those of small banks, but within each group the basic approach has been a me-too game of marginal improvements. Current offerings' homogeneity may render banks vulnerable to an aggressively innovative competitor, especially given relatively short development cycles.

So how can banks differentiate themselves to boost both customer loyalty and their brands? Unique offerings are obviously a good start. The key principle is high-value-added innovation, whether in personal financial management tools, biometric authentication, location sensing technology, or areas beyond.

Figure 1: Customers' use of mobile banking services



Source: Deloitte Centre for Financial Services

But feature innovation can only go so far toward winning customer loyalty, and its advantages may be transient in the fast-changing world of mobile technology. In the longer term, differentiating the mobile experience should be the strategy. Using analytics to draw insights from customer data and facilitate relevant, contextual interactions may raise customer engagement.

Monetising mobile: Not whether but how

To date, most banks have seen mobile primarily as a way to save on costs. Given the still-limited functionality of mobile apps, this focus makes sense. But as banks boost usage and invest in differentiation, they may also be able to generate new revenues.

At present, many bank customers say they are unwilling to pay for mobile banking services, perhaps due to limited understanding of its advantages. In our survey, 74 percent of respondents said they are not willing to pay any fees at all for mobile services. However, 27 percent of customers said they would be willing to pay for more "complex" services, possibly indicating a major opportunity.

The logic is simple: customers' willingness to pay depends on the value they perceive in the service. If more high value-added services are offered, customers may be less price-sensitive. The greater the value provided by the mobile experience, and the greater advantage banks take of mobile's unique capabilities, the greater the ability banks will have to monetise mobile.

Looking ahead: Making the transition to the post-channel world

Maintaining a seamless experience within the mobile ecosystem should be a priority. The expansion of mobility to wearable technology and the Internet-of-Things demands a device- and platform-agnostic approach to mobile banking. This strategy is consistent with banks' larger long-term goal: achieving the fluid integration of mobile and other channels. With its unique attributes, mobile has singular potential to break down banks' siloed approach to customers. We are nearing a world in which the sensing and communication capabilities of mobile technology allow phones, tablets, and other devices to become integral to every customer interaction; banks should already be actively investigating and investing in these technologies to create a superior and differentiated customer experience.

For the full version of our point-of-view, please visit our Financial Services pages at www.deloitte.com/sg.

Raising the bar on customer engagement

Mobility and customer engagement begin with awareness, then trust

Customer engagement is increasingly becoming a key focus area for financial services companies. The reasons are quite obvious. Few would doubt that engaged customers translate to greater economic value: customers who are more engaged tend to be more loyal and, as a result, more profitable.

But a key obstacle for companies is that consumers have become less trusting and more demanding. The financial crisis, in particular, eroded consumer trust across the financial services spectrum. And although public perceptions have improved somewhat since then, "the need to rebuild trust through performance is increasingly apparent."[1]

So in an age where attention spans are short and competition for mindshare intense, how can financial services companies build and enhance customer engagement?

The digital channel could hold substantial promise in this regard. Evidence is mounting that consumers who use mobile devices for their interactions with service providers are also more likely to have deeper engagement.[2] But how can financial services companies proactively elevate customer engagement beyond the existing boundaries offered by current mobile experiences?

We posit a four-step model of mobile customer engagement. The first step is to generate awareness of a company's mobile offerings; the second step is for the consumer to adopt them. The third step is consistent usage – that is, once a mobile offering (an app, for instance) is adopted, it has to be used on a regular basis. The fourth step is to achieve a deeper, more meaningful engagement with customers through mobile connections and services.

Getting on the map: Generating greater awareness and usage of mobile apps

Lack of awareness is a major barrier to adoption for at least two of the three financial sectors. For example, according to a recent Deloitte survey, 65 percent of survey respondents with a life insurance policy were not even sure whether their carrier offered a mobile app. The same can be said for 63 percent of those with homeowner's or renter's insurance, as well as 57 percent of auto insurance consumers. And nearly half of survey respondents were not sure whether their mutual fund, retirement account, or investment account providers offer mobile apps.

Banks have achieved greater awareness and usage at this point. In fact, 63 percent of smartphone users had interacted with their bank via a mobile app, compared with less than half that percentage for insurance and investment management. As for value, 39 percent of those surveyed characterised the ability to deal with their bank on a mobile device as extremely or very important, versus only 23 percent for investment-related activities and just 19 percent for insurance.

The imperative for mobile offerings

This Southeast Asia perspective was contributed by Mohit Mehrotra (momehrotra@deloitte.com), Executive Director, Consulting, Deloitte Southeast Asia.

The digital revolution has been the centre of attention in the financial services industry and will continue to be. We are in an era of digitisation, where the digital natives in ASEAN will spend more than the baby boomers, clearly providing a fascinating opportunity for banks. While on one hand "The software is eating the world" (Marc Andreessen), on the other hand banks are still working through customisation of their mobile offerings to address the key needs of its clients. Many of the mobile offerings today are largely around replacement of their internet based offerings. Banks have a vital role to play in developing innovative digital propositions that will help them develop emotional connection with digital natives and generate greater value for them. It also helps the banks in some economies enhance financial inclusion and accelerate the social and economic impact.

1 Edelman Trust Barometer, Trust in financial services, http://www.edelman.com/insights/intellectual-property/2014-edelman-trust-barometer/trust-inbusiness/trust-in-financial-services/, accessed April 11, 2014.
2 Joel Schectman, "In mobile, customer engagement more important than sales," Wall Street Journal CIO Journal, September 10, 2013.

This may in part be attributable to the nature of basic banking versus other financial services, with bank customers making inquiries and initiating transactions more regularly. But the twofold challenge for all financial sectors remains: how to increase the number of mobile interactions with consumers, as well as how to initiate and maintain deeper engagement via mobile devices by offering more sophisticated capabilities.

If they haven't already done so, companies should also be training client-facing staff to continually point out and remind customers about the mobile services at their disposal, especially since mobile adoption could spare such client-facing personnel the burden of performing many routine functions or responding to frequently asked questions. But even if greater awareness is achieved, adoption could still be a problem for many financial services companies due to technical challenges related to the devices themselves and the wireless networks they tap, as well as psychological misgivings arising from widespread concerns about privacy and security.

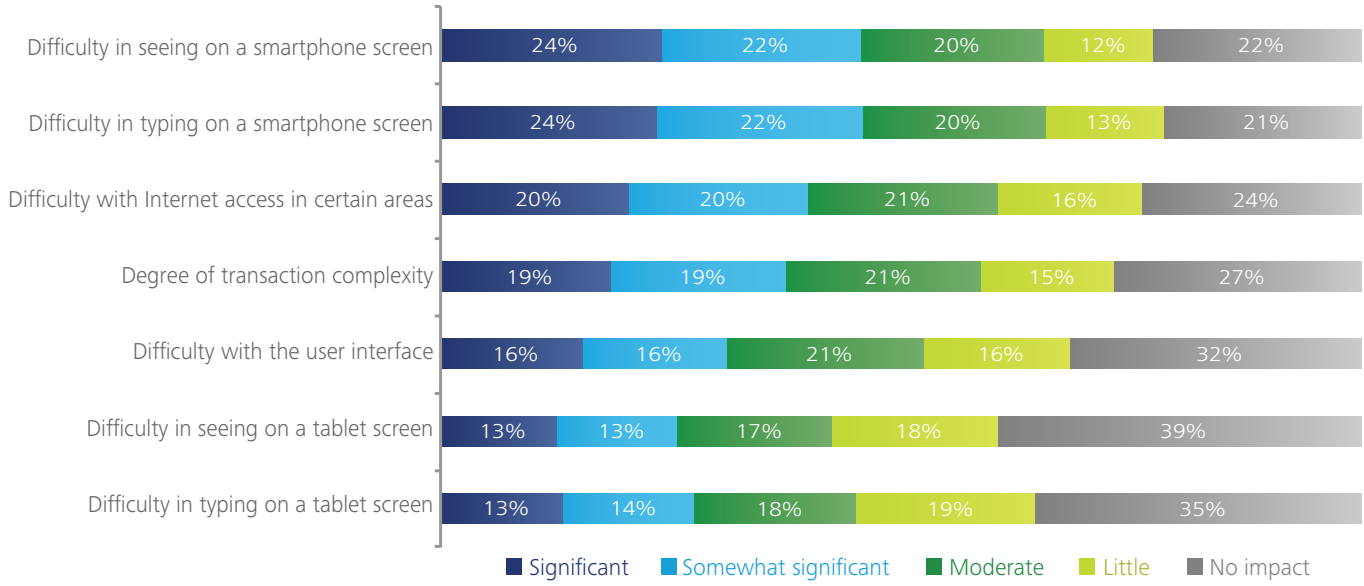
Overcoming obstacles to usage

Mobile technology offers the convenience of access on the run, from virtually any location. In addition, many people are using mobile devices for a variety of purposes in the comfort of their own homes, working their TV remote control with one hand and a mobile device with the other (if they are not already watching a programme or playing a game on their smartphone or tablet).

Yet for many consumers, when it comes to conducting financial services over mobile devices, the advantages and conveniences offered by smartphones and tablets are being trumped by more negative considerations about the devices themselves and data security.

For instance, one in four survey respondents said that the difficulty of seeing and typing on a small smartphone screen was a significant limitation that discouraged them from using their mobile device more often (Figure 2). Such factors – which were much less of a concern for those using tablets – were also cited, particularly by older consumers, as by far the two most significant barriers to using smartphones to conduct their financial services business.

Figure 2: Limitations in using mobile devices[3]



Source: Deloitte Centre for Financial Services

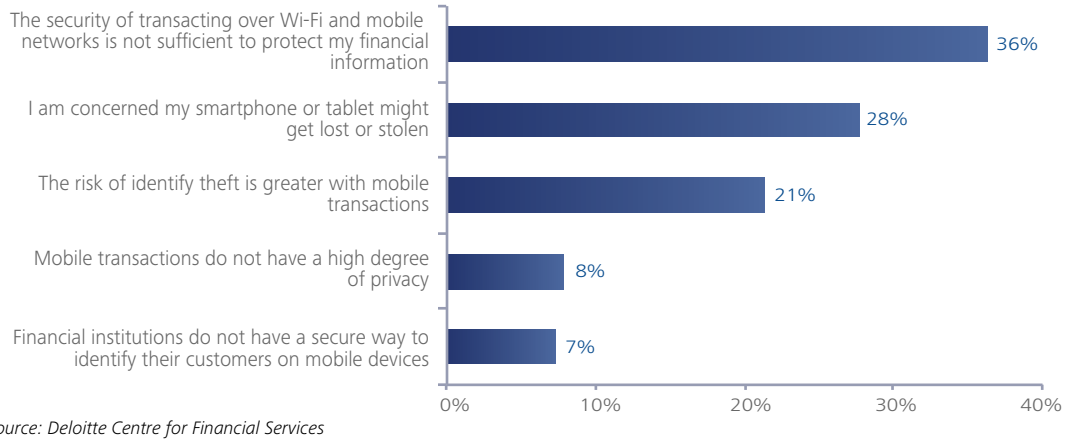
3 Please note that the total percentage in the charts may not add to 100 percent due to rounding error.

Meanwhile, 61 percent of those who do not regularly use mobile devices for financial services cited security issues as the prime reason. This is 22 points higher than the percentage citing the next most common reason (a preference for doing such business in person or with a human being over the phone).

A little over one-third of respondents were insecure about transacting financial services business on mobile devices because they do not trust the security of the Wi-Fi and mobile networks transmitting their data. Meanwhile, when asked about their primary security concern, 28 percent cited the risk of their mobile device being lost or stolen, and 21 percent cited the risk of identity theft (Figure 3).

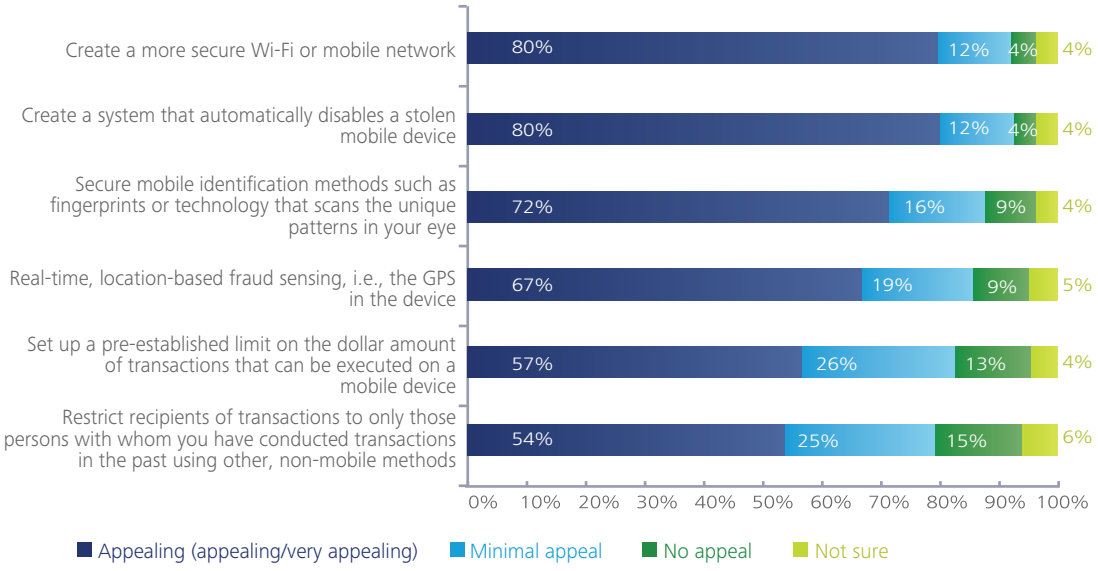
To boost adoption and set the stage for more ambitious applications, companies will likely have to take tangible steps to reassure consumers about the security of their mobile financial transactions. Along those lines, 80 percent of those surveyed would like the ability to remotely disable a lost or stolen device, while 72 percent would appreciate the use of biometric identification (such as fingerprints or eye scans) to enable a device for financial services transactions. For banking security, over half of our respondents like the idea of preclearing a limited number of people who could receive funds in a mobile payment, as well as setting a dollar limit on such transactions. Two-thirds supported leveraging the mobile device's GPS for real-time, location-based fraud sensing (Figure 4).

Figure 3: Factor most influencing security concerns related to mobile devices



Source: Deloitte Centre for Financial Services

Figure 4: Appeal of different factors mitigating mobility security concerns



Source: Deloitte Center for Financial Services

Implementing these and other concrete security measures, then calling attention to such efforts in advertising and social media campaigns designed specifically to address such concerns, could perhaps help overcome lingering consumer hesitations about accessing personal financial information or transacting financial business over smartphones and tablets.[4]

Targeting marketing to mobile prospects

Another way to widen adoption and expand usage of mobile financial applications might be to target different audiences with different messages, focusing on whatever issues concern each segment the most.

To start out, a two-pronged strategy based on age might be in order. Older prospects could receive mobile pitches about a company's efforts to alleviate security concerns for routine transactions. The messaging for younger prospects could be more focused on using mobile to create a virtual community around financial services issues, as well as to take advantage of advanced, value-added interactive capabilities.

Indeed, age was the most significant differentiating factor among the consumers in our survey. Younger respondents, in general, were more aware of the availability of mobile apps in financial services, as well as more likely to use them.

Still, while younger consumers may be more receptive to services via mobile devices, that does not mean they will be an easier group to recruit and retain as customers simply because of the availability of financial apps. Indeed, this segment is likely to be more demanding in their expectations for mobile financial services, given their mobile service experiences with other industries employing more advanced apps.

In addition, while older consumers might be a tougher sell for mobile services because of their deeper concerns about security and the ease of using smartphones, this segment, broadly speaking, has the most to bank, invest, and insure. Targeted efforts to communicate how mobile security and usage issues might be overcome are therefore critical.

For the full version of our point-of-view, please visit our Financial Services pages at www.deloitte.com/sg.

4 Fumiko Hayashi, "Mobile payments: What's in it for consumers?" Federal Reserve Bank of Kansas City, Economic Review first quarter 2012, http://www.kansascityfed.org/publicat/econrev/pdf/12q1Hayashi.pdf.

Lessons from the front lines
E-Commerce & Online payments

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many C-suite executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organisation do to shore up its defences and protect itself from cyber-threats?

A common myth is that cyber-attacks only happen to certain types of organisations, such as high-profile technology businesses. However, the cold, hard truth is that every organisation has valuable data to lose. In fact, the attacks that happen most frequently are completely indiscriminate – using scripted, automated tools that identify and exploit whatever weaknesses they happen to find.

Cyber-attacks can be extremely harmful. Tangible costs range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for injured parties. However, what might hurt even more are the intangible costs – such as loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, loss of integrity due to compromised digital assets, and overall damage to an organisation's reputation and brand – all of which can send an organisation's share price plummeting, and in extreme cases can even drive a company out of business.

Being resilient to cyber-risks starts with awareness at the board and C-suite level; a recognition that at some point your organisation will be attacked. You need to understand the biggest threats, and which assets are at greatest risk – the assets at the heart of your organisation's mission.

Who could potentially target your organisation, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack (see Table 1), and what is the potential impact to your business?

Table 1: Frequency of incident classification patterns from 1367 breaches during 2013

Incident classification pattern	Percentage
Point of Sale system intrusions	14%
Web app attacks	35%
Insider misuse	8%
Physical theft/loss	<1%
Miscellaneous errors	2%
Crimeware	4%
Card skimmers	9%
Denial-of-service attacks	<1%
Cyber-espionage	22%
Everything else	6%

Source: Verizon 2014 Data Breach Investigations Report

Questions such as these can help determine how advanced and persistent the cyber-threats to your business are likely to be. This insight allows you, as a C-suite executive or board member, to determine your organisation's risk appetite and provide guidance that helps internal and external security professionals reduce your risk exposure to an acceptable level through a well-balanced cyber-defence.

Although it isn't possible for any organisation to be 100 percent secure, it is entirely possible to use a mix of processes for prevention, detection, and response to keep cyber-risk below a level set by the board and enable an organisation to operate with less disruption.

The evolving cyber-threat landscape

This section was contributed by Thio Tse Gan (tgthio@deloitte.com), Executive Director, Enterprise Risk Services, Deloitte Southeast Asia.

In recent years, the business and technology innovations that financial institutions are adopting in their quest for growth, innovation, and cost optimisation have presented heightened levels of cyber-risks to their organisations. For example, the continued adoption of Web, mobile, cloud, and social media has compounded the opportunities for attackers.

Similarly, the waves of outsourcing, offshoring, and third-party contracting driven by cost optimisation objectives have further diluted institutional control over IT systems and their respective access points. These developments have likely introduced complexities into the technology ecosystem that potentially increases the vulnerability of critical systems used by financial institutions.

Financial institutions should consider raising their level of preparedness and evolve towards a proactive cyber-risks management paradigm that strives to achieve three fundamental qualities:

- **Being secure** against known threats through risk-driven investment in foundational, preventive controls, and policies;
- **Being vigilant** by improving the ability to detect emerging threats and anomalous patterns amidst the highly complex and data-saturated environment;
- **Being resilient** to enable the organisation to recover from attacks as quickly as possible and minimise both direct and indirect damages.

Exhibit 1: Improving cyber-security with a "secure, vigilant, and resilient" strategy

Traditionally the focus has been on being secure. However, the evolving cyber-threat landscape may necessitate a shift to a more dynamic approach and well-rounded cyber-security capability.

SECURE
Enhance risk-prioritised controls to protect against known and emerging threats and comply with industry cyber-security standards and regulations

VIGILANT
Detect violations and anomalies through better situational awareness across the environment

RESILIENT
Establish the ability to quickly return to normal operations and repair damage to the business

Source: Deloitte Centre for Financial Services analysis

For many financial institutions, their typically IT-risk management processes can and should evolve into executive-driven cyber-risk management programmes that are integral to the strategic business planning. The imperative to transform is a strategic business issue and the financial institutions that master this new approach could be at the forefront of the industry. By incorporating a more agile cyber-risk management approach, they would be in a leading position to effectively manage the threats and harness the full potential of the digital evolution.

Cyber threats: e-commerce & online payments

One of the most common attacks in e-commerce and online payments is a database breach. Often, such attacks result in a loss of customer data, including names, physical addresses, phone numbers, e-mail addresses and payment information. Since trust is especially important in e-commerce, the loss of customer data can be very damaging to an online company's reputation and business performance. The impact of a breach can go far beyond reputation damage, depending on where in the world it occurred. A number of US states have already instituted breach notification laws, and the EU is expected to follow shortly. Such laws require organisations to come forward and publically admit they were breached. The EU directive also includes heavy fines.

Online payment systems are another vulnerable area that is often attacked. The ability to accept payment is critically important for online businesses, since it is one of the last steps in a customer's purchase journey. As such, the financial impact of a payment system attack can be enormous, depending on its duration. After all, if customers can't pay, they can't buy.

Most e-commerce sites outsource payment processing to a variety of third-party providers that promise high availability of their payment services. However, these providers are increasingly being targeted with denial-of-service attacks, particularly by hacktivists that want to disrupt an organisation in a highly visible way. Payment-related attacks are also appealing to criminals looking for financial gain. Saving a customer's credit card data in an internal database might seem like a good way to make the shopping process more convenient, but it creates an attractive target for cyber-criminals.

Payment processing vendors are even more attractive to attack, since the potential for a big score is much greater. In the brick-and-mortar world, cyber-criminals have developed a variety of techniques for skimming credit cards at Point of Sale (POS) terminals and ATMs. Also, they have developed a wide range of attack vectors targeted directly at online payment vendors. Some of the most sophisticated attacks use a combination of online and traditional physical techniques to increase their effectiveness.

Attacks on a payment vendor can be just as damaging to a company's reputation as attacks that target the business directly, since most customers don't see a distinction between an organisation and its service providers.

For the full version of our point-of-view, please visit our Financial Services pages at www.deloitte.com/sg.

Case study 1: Hacktivists strike back with a vengeance

Organisation
A very large financial services firm whose core global business is processing credit card transactions.

Scenario
A popular protest turned into cyber-terrorism with a call-to-action from a politically motivated hacker collective. Together, thousands of people initiated a large denial-of-service attack on the company's network, making its services unavailable to clients.

Attackers and motivation
The attack was motivated by the company's decision to block payments to a well known website based on claims that the site's activities were illegal. This decision caused a worldwide commotion among the website's supporters. Popular support for the cause – combined with low technical requirements to participate – resulted in a large-scale attack.

Techniques used
To make the attack as successful as it was, the hackers recruited a large numbers of volunteers to help. All participants installed special attack software on their computers, which together formed a single large botnet. The software was specifically designed to perform a large distributed denial-of-service attack (DDoS) on the company's network. Instructions were sent via chat telling all of the computers in the botnet to start attacking the company's network. Due to the large number of people involved in the attack, the company's payment services quickly became unavailable or highly inaccessible for 10 hours.

Business impact
Direct costs of the attack have been estimated at more than $3 million. But the incident's overall impact was even greater, showing how cyber-protests could be used to damage organisations and influence their behaviour. Since the attack, other organisations within the sector have been targeted for protest by the same group.

Case study 2: Thieves use stolen data to create their own credit cards

Organisation
A large financial services firm that provides electronic transaction processing worldwide.

Scenario
A group of criminals broke into the company's systems and over the course of a year stole magnetic stripe data for approximately 7 million credit cards. They then created fake credit cards by programming the stolen data onto cheap prepaid cards, which were later used to purchase expensive items such as computers and televisions.

Attackers and motivation
The attackers were motivated by financial gain. The careful target selection and sophisticated techniques used for the attack suggest the involvement of a well organised cyber-criminal group.

Techniques used
Attackers infiltrated a crucial part of the payment processing infrastructure containing magnetic stripe data, which was then exported to create duplicate credit cards that were later used for fraudulent transactions.

Business impact
The company revealed that the data breach cost an estimated $90 million, which includes fraud losses as well as fines, costs associated with the investigation, charges from card networks and client aftercare. The company's reputation also took a lot of damage, both from consumers and from clients within the payment card networks.

13

Banking on Tax

Income tax treatment of hybrid instruments in Singapore

This article was contributed by Michael Velten (mvelten@deloitte.com), Partner, Tax, Deloitte Southeast Asia.

Income tax treatment of hybrid instruments in Singapore

The Inland Revenue Authority of Singapore (IRAS) recently issued guidance on the income tax treatment of hybrid instruments in Singapore (the Guide). Prior to this guidance, there have been no specific provisions in the Singapore Income Tax Act (ITA) on the character of hybrid instruments for tax purposes (i.e. whether a hybrid instrument is debt or equity for tax purposes).

The one exception is the 2014 Singapore budget amendment to treat Basel III Additional Tier 1 (AT1) capital instruments (other than shares) issued by specified Singapore-incorporated banks and their holding companies as debt for tax purposes.

IRAS Guide: Income tax treatment of hybrid instruments

Briefly, where the legal form of a hybrid instrument issued by a Singapore-based issuer is not indicative of the legal rights and obligations, IRAS will adopt a 'combination of factors' approach to determine the tax treatment of an instrument. Under this approach, the characteristics of a hybrid instrument are examined and considered in entirety.

Factors considered by the IRAS (with the debt/equity inference in parenthesis) include:

- Investor acquires a shareholding and residual interest in the issuer (equity)
- Investor acquires a right to participate in the issuer's business (equity)
- Instrument confers the investor with voting rights (equity)
- There is a fixed repayment date in a reasonably foreseeable future and repayment is not conditional on business performance of the issuer (debt)
- There is no fixed repayment date, although there is incentive for the issuer to redeem the instrument, such as a step-up feature (debt)
- Distributions are cumulative and payment is not conditional on business performance (debt)
- Investor has an unconditional right to enforce the payment of a distribution and repayment of the principal amount (debt)
- Relevant regulatory authorities in Singapore regard the hybrid instrument as debt (debt)
- The right of the investor to repayment of principal is subordinated to that of the general creditors or to the holder of subordinated debt of the issuer (equity)
- The investor is required to bear current or future losses of the issuer by way of either a write-down of the principal amount of the instrument or conversion to ordinary shares of the issuer (equity).

The Guide does not discuss the weight allocated to each factor, nor the tax treatment of instruments that have already been issued in the Singaporean market (e.g. perpetual securities). However, without the recent budget change to the treatment of AT1 capital issued by a local Singapore bank, such an instrument should be expected to be equity based on the above tests.

To characterise a hybrid instrument issued by a foreign-based issuer, IRAS will examine the above factors. IRAS notes in the Guide that it will also consider the characterisation of the instrument in the country of the foreign issuer and that "the use of this guide may be limited by new forms of hybrid instruments as well as changes in tax treatments adopted by foreign tax jurisdictions which may have an impact on the Singapore income tax consequences".

In doing so, IRAS is seeking to address potential mismatches in the tax treatment of hybrid instruments across jurisdictions.

The position articulated by IRAS in the Guide is not the law and taxpayers may appeal to the courts if they do not agree with IRAS' position. For taxpayers that require certainty, an advance ruling may be sought from IRAS.

Income tax treatment of Basel III AT1 instruments
Broadly speaking, AT1 capital instruments, other than shares, issued by specified Singapore banks and their holding companies will be treated as debt for income tax purposes with effect from the 2015 year of assessment (i.e. from 1 January, 2014). Distributions on these instruments will be tax deductible. Tier 2 instruments, other than shares, are currently regarded as debt for tax purposes and will continue to be regarded as debt.

This treatment does not extend to AT1 instruments issued by Singapore branches of foreign banks. These branches are not required to comply with MAS Notice 637, which is issued to banks incorporated in Singapore and sets out directives on their risk-based capital adequacy requirements. As such, hybrid instruments issued by these branches are likely to be subject to the 'combination of factors' approach discussed above.

Other developments
A new section 14X is to be introduced into the ITA (via Income Tax (Amendment) Bill 2014). The proposed section 14X provides for the deduction of expenditure incurred by a person for the purpose of complying with any local or foreign legal or regulatory requirements, if the expenditure is not capital in nature and is incurred for the purpose of any business from which the person's income is acquired. The new section 14X will apply from the 2014 year of assessment.

The income tax treatment of Basel III AT1 instruments may lead to a scenario where hybrid instruments with materially similar terms and conditions have different tax treatments based on the status of the issuer.

IFRS 9 industry insights

Banks required to adopt new loss model and changes to financial asset classification

What has happened?

The International Accounting Standards Board (IASB) has issued the final version of IFRS 9 *Financial Instruments* incorporating amendments to the classification and measurement model for financial assets and a new expected loss impairment model. IFRS 9 is the replacement to IAS 39 *Financial Instruments: Recognition and Measurement* and is effective for reporting periods beginning on or after 1 January 2018, with earlier application permitted (subject to local endorsement requirements).

The project to replace IAS 39 has been undertaken in stages. The IASB first issued IFRS 9 in 2009 with a new classification and measurement model for financial assets followed by requirements for financial liabilities and derecognition added in 2010. Subsequently, IFRS 9 was amended in 2013 to add the new general hedge accounting requirements. The final version of IFRS 9 issued in July 2014 supersedes all those previous versions although they remain available for early adoption for a limited time.[5]

Implications for the banking and securities sector

The changes to financial instrument accounting are likely to have the greatest impact on banks and other financial institutions. Below is a high-level discussion of some of the key impact areas arising from the amendments to the classification and measurement model and the new expected loss impairment model.

Amendment to classification and measurement of financial assets

The new fair value through other comprehensive income (FVTOCI) classification is a mandatory classification that is applied to assets that pass the contractual cash flow characteristics test[6] but are held within a business model whose objective is achieved by both holding to collect contractual cash flows and selling the assets. A fair value option is available on initial recognition as an alternative to FVTOCI if measuring the asset at fair value through profit or loss (FVTPL) would eliminate or reduce an accounting mismatch.

Less profit or loss volatility for banks

Compared to the original requirements in IFRS 9, the introduction of the FVTOCI category can result in some of those assets that would have been measured at FVTPL (due to failing the business model test for amortised cost measurement) to be at FVTOCI. This could result in less profit or loss volatility for banks than would have otherwise arisen. For example, liquidity portfolios where frequent and significant sales arise in order to demonstrate the liquidity of the investments would not have met the requirements for amortised cost measurement but could be eligible for the FVTOCI classification.

Analysing business models

Banks will need to distinguish their business models to determine which are those with an objective to "hold to collect contractual cash flows" and which are to "both hold to collect and to sell". In some cases this may require significant judgment and will need to be tackled early on in the implementation. In particular, if a bank wishes to designate assets that would meet the classification requirements for FVTOCI at FVTPL, it must do so by the date of initial application (i.e. if these assets are identified as meeting the FVTOCI criteria after the date of initial application, the fair value option will no longer be available).

5 The previous versions of IFRS 9 may be early adopted if the entity's relevant date of initial application is before 1 February 2015

6 The contractual cash flow characteristics test is passed if the financial asset solely consists of a return of principal and interest on the principal outstanding. If the financial asset passes this test it will be measured at amortised cost if it is held in a business model that collects contractual cash flows or FVTOCI if the business objective is to both collect the contractual cash flows and sell the asset. If neither business model applies, or the fair value option is invoked, the asset is measured at FVTPL.

FVTOCI vs AFS

The FVTOCI classification differs from the available-for-sale (AFS) classification under IAS 39 as FVTOCI is not the residual category (instead FVTPL is) and most importantly, expected losses are applied in measuring impairment. As the AFS classification is used extensively by banks, for example for liquidity portfolios, the impact of this different treatment will need to be considered.

New expected loss impairment model

Wider scope

IFRS 9 introduces a new expected loss impairment model which replaces IAS 39's incurred loss model. It is applied to:

- Debt instruments held measured at amortised cost or FVTOCI
- Written loan commitments and written financial guarantee contracts where IFRS 9 is applied (unless they are measured at FVTPL)
- Lease receivables within the scope of IAS 17 *Leases*
- Contract assets within the scope of IFRS 15 *Revenue from Contracts with Customers* (i.e. rights to consideration following transfer of goods or services that the entity has transferred to a customer when that right is conditioned on something other than the passage of time, for example, the entity's future performance)

The main difference in scope to IAS 39 is that certain loan commitments and financial guarantee contracts are assessed for impairment under IFRS 9, rather than IAS 37 *Provisions, Contingent Liabilities and Contingent Assets.* This makes sense given loan commitments and financial guarantee contracts are similar and that a forecast credit loss on a potential drawdown on a loan will now be measured the same way as if it is drawn down.

A single model

Furthermore, the single model approach will mean that both debt instruments measured at amortised cost and those measured at FVTOCI will have the same loan loss allowance despite the different measurement basis on the balance sheet. This will result in more comparable loan loss results amongst banks that have similar assets but classified differently between amortised cost and FVTOCI.

Day-one provision

The loan loss allowance is measured one of two ways[7]:

- 12-month expected loss allowance
- Lifetime expected loss allowance

Generally, when a financial asset is first recognised a 12-month expected loss allowance is recognised. Hence, when a bank originates or purchases a loan or debt security measured at amortised cost or FVTOCI a day-one provision with a debit to profit or loss will be recognised. This day-one loss could have a more significant effect on the performance of a bank that is growing its loan book since with more loans being recognised than derecognised, the overall loan loss allowance will increase (everything else being equal). This effect on profit or loss, as well as the impact of reduced net assets, will need to be evaluated for some banks (e.g. the knock-on consequences for regulatory capital, the pricing of loan products and messaging to stakeholders).

7 With the exception of purchased credit-impaired assets where expected losses are incorporated into the expected cash flows from which the (credit-adjusted) effective interest rate is derived which is the same treatment as under IAS 39

Monitoring credit risk migration

When there is a significant increase in credit risk the loss allowance moves from a 12-month expected loss allowance to an allowance for lifetime expected losses. This new, earlier, trigger for recognising impairment losses will mean banks will have to establish appropriate systems and processes for identifying when there has been a significant increase in credit risk. This will involve assessing the availability of data and information about the credit risk of the items in scope of the model and also consider how that data and information can be tracked to identify when credit risk has increased significantly from inception of the exposure.

Measuring expected losses

Loss allowances will be measured on a probability-weighted basis, discounted by the effective interest rate (or an approximation thereof), based on information regarding past events, current conditions and a reasonable and supportable forecast of future economic conditions that is reasonably available without undue cost and effort. This measure of the loan loss allowance will again demand the use of data and information not previously used under IAS 39.

As with the data used for monitoring credit risk, much of the necessary information would exist within a bank, however, the challenges will be around the accurateness and reliability of such data given that some will not have been used for accounting purposes (rather they would be used for credit risk management or regulatory reporting).

Transparency

Given the number of judgments and assumptions required to apply the model, IFRS 7 *Financial Instruments: Disclosures* requires extensive disclosures to accompany the accounting. These disclosures will provide transparency on the application of the model and is likely to be used to compare banks' provisioning amongst peers and track changes in provisions from year to year. Therefore the messaging of these enhanced disclosures is likely to require some advance consideration.

Transition

When IFRS 9 is first applied, both the classification and measurement, and impairment requirements are to be applied retrospectively, with an option not to restate prior periods.

In addition to the exception from restating comparatives, if at the date of initial application, determining whether there has been a significant increase in credit risk since initial recognition would require undue cost or effort, a lifetime expected loss allowance is recognised until the financial instrument is derecognised (unless the credit risk is low at the reporting date). The effect of this is that an absolute measure of credit risk at the reporting rate dictates the recognition of lifetime expected losses rather than a relative measure comparing to initial recognition. The practical benefit of this approach for a bank would have to be weighed against the consequence of recognising a higher provision on transition and the burden of having two impairment approaches running parallel for future periods.

For the full version of our point-of-view, please visit our Financial Services pages at www.deloitte.com/sg.

Why less is more in Management Information

This article, written by Ashley O'Reilly (asoreilly@deloitte.com), Manager, Consulting, Deloitte Southeast Asia, first appeared in the Asian Banking & Finance magazine on 7 August 2014.

Banking executives are generally frustrated by the lack of efficient and effective Management Information (MI) that they receive to run their businesses in Asia. Sources of this frustration include MI duplication which often exists across business functions; laborious and error-prone manual production of MI; production of reports that lack focus or insight; gaps in MI such as missing HR and/or sales data; and poor MI storage, governance, and delivery.

Banking executives in Asia want to frequently receive summarised snapshots of relevant and standardised MI, governed by a structured distribution process that incorporates a formalised feedback loop to all business lines. There is low overall consumer satisfaction with MI within the Asian banking industry driven by three attributing themes: Inconsistent MI, Untimely MI, and Irrelevant MI. Banking executives should receive appropriate MI to make effective decisions and run their businesses without wasted effort on redundant MI activities.

Inconsistent MI and a lack of 'one version of the truth' is a recurring concern among Asia-based banking executives. A bank in Singapore suffers from poor MI quality which has led to a lack of trust during data interpretation. The producers of MI must understand the business and reasons why core information is required.

Consistency in the approach and presentation of MI is also important to ensure that data is analysed and used correctly. Business departments require tools and processes to ensure that the data they provide to executives is consistent (e.g. business performance results as calculated by Finance and independently by geographical operations departments). A multitude of independent MI producers leading to a lack of a single source of truth is a recurring cause of MI inconsistency across the market.

We frequently hear about data not being readily available and unreliable processes and systems for the conveyance of MI. Some banks in Singapore manually load MI components into systems and subject data to manual manipulation (e.g. to resolve reconciliations) which delays MI and subjects it to error risk. Data integrity steadily decreases when figures are manipulated by numerous people.

There is also a strong correlation between the value of MI and the rate in which it is received by its interpreters due to quick fluctuations in exposures, exchange rates, and so forth. Furthermore, if related MI is not delivered at the same time, its meaning can be diluted driving further inefficiencies.

A key contributing factor causing untimely MI is there being too much data produced and disseminated. Producers must understand the usefulness of the reports they are producing so that they can focus on the timely production of MI that increases business performance and/or better supports the making of important decisions.

MI consumers tell us that they are often required to sift through irrelevant data in order to find MI that meets their strategic needs. Occasionally, executives receive raw data and not the organised MI they require to quickly and easily digest and analyse.

Banks in Asia need to produce less data reports and more analytically enabled MI. MI and data should be governed in such a way that ensures standardisation of geography, country, product, etc. reporting.

Reviews of bespoke MI produced by most banks reveal that not all legacy MI is actively used to manage businesses. Key indicators of potentially irrelevant MI include MI lacking forward forecasting; reports containing duplicated data; geography specific reports with no link to overall regional strategy; raw data dumps; etc.

The solutions to MI effectiveness and efficiency issues are not all costly and time-consuming. Certainly central data warehouses improve MI production and interpretation dramatically, however other more immediately achievable opportunities to improve MI production and delivery exist.

All functions within banks should understand the MI needs of their executives. Identifying critical MI and rationalising non-critical reports and associated processes is equally important.

Banks need to assess the effectiveness and efficiency of their critical reports; identify data, structural and other content design improvements, and tailor solutions to improve MI automation, accessibility, and usability. Once solutions are implemented, banks must determine and implement appropriate on-going MI governance.

By 2020, the digital universe will be 9 times bigger than it is now.

Take a second and try to imagine every piece of digital information you have ever seen. Now imagine that multiplied by all the people in the world and add a factor of time… You still are nowhere near imagining the estimated 4ZB (zettabytes) of data in the digital universe today.

That's right: zettabytes. One sextillion bytes or a billion terabytes, if that helps. But data growth has been enormous, growing as much as 50% year-on-year as we move towards the most common estimate of around 35ZB of data in 2020.

Imagine all the information contained in that much data and what you could do with it if you just knew how… then you'll understand why data analytics is often said to be 'the next big thing.'

Want to know more? Come talk to Deloitte and decipher the future together.

Deloitte.