# Innovation through mobility: Customers first or employees first?

Harnessing the potential of **Mobile and Banking**

Confidence in a connected world. Symantec.

# Contents



# Introduction

Banks are in an enviable as well as challenging position. Despite the increasing dilution of the banking ecosystem, traditional banking institutions maintained a strong position until the 2008 financial breakdown led to a shift in trust and opened up the sector to **new entrants**. This coincided with new technology becoming available and the rise of innovative partnerships between banks and businesses including service providers, e-commerce and payment providers.

As a result, the competitive landscape and financial crisis have now closed in, demanding **innovation** and cost control to survive. Meanwhile, legislation is forcing investments in risk management and elevating levels of control in an already heavily regulated industry.

This presents a great opportunity to overhaul traditional banking practices. Mobile technology, in particular, is opening up new capabilities and **new channels** for banks to the extent that it is starting to be referred to as the 'third platform'.

The true innovative potential for mobile technology occurs when it is viewed not just as an extension of the web, but instead as a means of developing operational abilities that would not be possible with other technologies.

However, integration of mobile technology is complex. It creates a new security perimeter which impacts on an organisation's overall security and risk strategy.

# Mobile technology is changing the way we do business

The world is going mobile. IDC believes that by 2016, worldwide smartphone shipments will reach 1.246 million units[1]. The impact on the banking industry is also increasing, with both employee and customer behaviour changing as mobile technology is incorporated into everyday life. Mobile data traffic is expected to grow 26-fold between 2010 and 2015[2].

### The impact on the banking industry

So what does this mean for the banking industry? On one hand, it is easier for employees and customers to quickly access information from **anywhere**. Many innovative services can be delivered on these new platforms and more applications are being released every day to support mobile behaviours. On the other hand, mobile devices introduce **new threats** and regulatory issues that expand beyond the PC world.


The fact that banking has traditionally been seen as a conservative institution does not mean that it can afford to be seen as such going forward. The competitive pressure is immense as new players, including online banks, niche banks, telecom operators and retailers are all looking to take market share in traditional banking services. Not only is this creating a need for innovation, but it is also becoming key for recruiting talent as the younger generations seek out agile and flexible employers where new technology flourishes.

### Customer behaviour is changing

Customer behaviour is driven by convenience, so even though banking customers are relatively reluctant to change provider, they will add accounts with a second bank that can offer additional or complementary services. The key challenge for banks is to **retain their customers** in a competitive and expanding banking ecosystem, as customers get other options the churn rate will inevitably increase if banks are not providing the services customers anticipate and expect.

The ability to offer client security on top of the bank's security solutions for access adds a layer of protection to banking services. This will become increasingly important as the mobile wallets and payments trend grows. At present, the mobile payments landscape is still largely fragmented with different initiatives being trialled across different countries. What is striking is that the cross-border initiatives to regulate and standardise have achieved very little in the past ten years, leading to local initiatives and solutions that have had very little impact on international standards.

## Capitalise on new businesses opportunities

Banks are already highly trusted to handle personal financial management. They hold customers' financial accounts and are established issuers of payment cards and other instruments. Existing payment infrastructures and services mean that security processes and systems are in place to do so safely.

As mobile payments gain importance, financial institutions are liaising with operators and handset manufacturers to provide mobile services to customers and partners.

**The need to adapt quickly to change**

Banks' legacy payment systems may present some challenges in adapting quickly enough to the fast pace of developments in mobile phones and services. Taking advantage of the opportunities as they arise will require innovation and flexibility. Issues such as: time to market, speed of execution, new security and authentication schemes will need to be addressed; as well as gaining a solid understanding of the business opportunities offered by mobile devices.

**The growth of multiple access channels**

Strategically, banks are moving to multiple channels and access, both as a cost reducer (moving services to the Internet minimises costly face-to-face interactions) and a growth contributor (upselling new services and increasing customer engagement).

*"New channels such as mobile and social networking sites are creating new risks for FSIs, and that 42% of institutions were planning to change data access controls internally"*

*Source: IDC Financial Insights Security Survey – FSIs Must Commit More Investment and Governance to IT Security as Risks Grow - May, 2011 - Doc # FIBA02T*

Branches are decreasing and their role is changing to advisory services rather than transactional and informational services. Continued investment in mobile and online banking is necessary in a competitive landscape where small online banks take market share through agile and innovative services.

**Worldwide Smartphone Operating System 2012 and 2016 Market Share and 2012-2016 Compound Annual Growth Rate**

| Smartphone OS | 2012 Market Share | 2016 Market Share | 2012-2016 CAGR |
|---|---|---|---|
| Android | 61.0% | 52.9% | 9.5% |
| Windows Phone 7/ Windows Mobile | 5.2% | 19.2% | 46.2% |
| iOS | 20.5% | 19.0% | 10.9% |
| BlackBerry OS | 6.0% | 5.9% | 12.1% |
| Others | 7.2% | 3.0% | -5.4% |
| **Total** | **100.0%** | **100.0%** | **12.7%** |

*Source: IDC Worldwide Mobile Phone Tracker, June 2012*

Financial services via mobile are among the most popular services and user behaviour demonstrates that mobile access (as well as online) contributes to a more frequent interaction. However, the adoption of mobile and online banking varies across countries. In Europe, Sweden and Holland were early adopters of digital channels, while countries such as Italy and Portugal still lag behind. In Asia, Singapore and Hong Kong have the top smartphone penetration rates, while other regions such as Australia are also showing high rates of adoption. When developing new mobile applications, banks also need to look at device adoption, with market shares predicted to change in the coming years.

The spread of online banking (and mobile banking) and also the level of security awareness will impact on strategy, as risks will be elevated when consumer security measures are low.

**The impact of social networks**

Many banks have started using social networks for marketing or customer information but using them for transactional services is still rare. The overall picture suggests that smaller banks are more aggressive in their use and traditional banks slower in adoption. The track record of online and mobile banking channels has proved customer engagement can be increased and suggests that social networks could boost this even more.

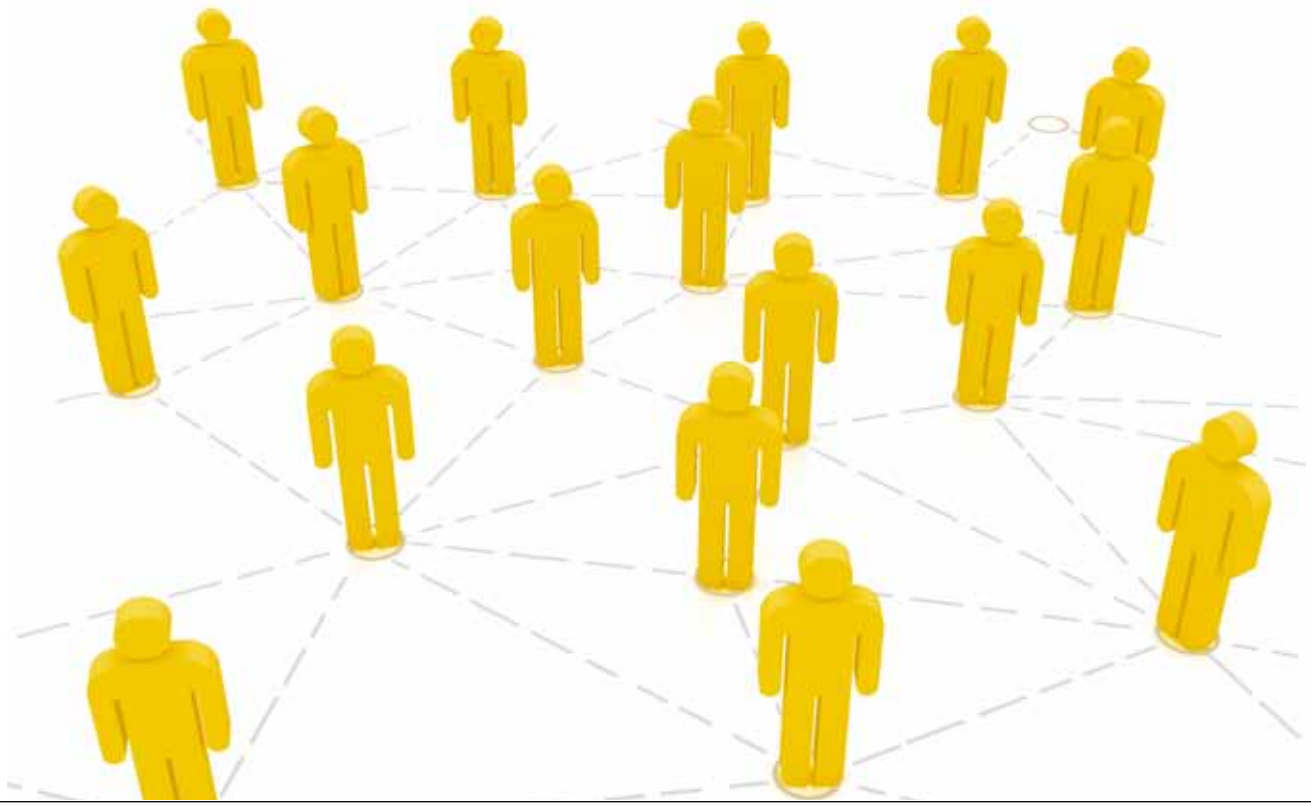
Social networks can also be viewed as a distribution channel. IDC research revealed that companies were predominantly using consumer social media tools in three ways[4]:

- To communicate with customers
- To create product or service awareness
- To acquire knowledge or ask questions about the customer

Financial institutions should view the use of social media as an enhancement to the customer experience value chain and as a channel to manage a virtual identity. As the services offered at branches are evolving to address more complex customer requests, online and mobile can offer a channel for real-time, always on, services.

However there are also risks related to using social networks, both internally and externally, and there needs to be a plan for the social objectives of the organisation.

Security concerns exist from customers at this phase of acceptance. However, First National Bank in South Africa has launched a service that allowed customers to transfer limited sums of money, in the form of pin-enabled vouchers, to their personal contacts on a social networking website. These vouchers could then be converted either into cash or prepaid airtime for mobile devices. This service demonstrates the possibilities that exist for local banks without the need to over-complicate offerings or risk exposing sensitive information.



## Bring Your Own Device – unleashing and enabling the bank employee

Employees are increasingly bringing their own smartphones, tablets or laptops to work and many companies are now offering employees an allowance or subsidy to buy their own computer equipment.

These trends, known as 'bring your own device' (BYOD), present a major challenge to IT departments who no longer control every device on the network. There is also the risk that a device owned by an employee might be used for non-work activity that exposes it to more malware than a device strictly used for business purposes only.

Although consumerisation and bring your own device aren't new concepts, a shift has occurred recently in how banks are approaching them. While Chief Information Security Officers (CISOs) and other bank executives remain wary of security issues surrounding the use of employee-owned mobile devices for work, they're increasingly embracing consumer IT within the enterprise as an opportunity to drive efficiency and innovation, as well as to increase employee (and customer) satisfaction.

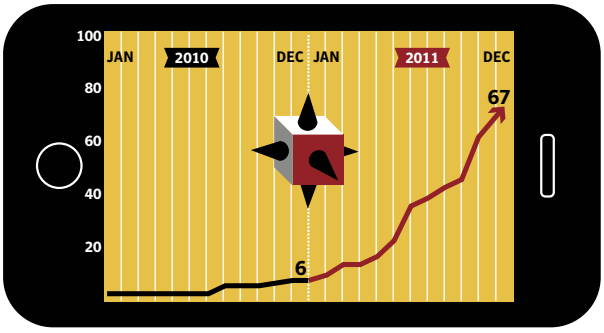
Forrester research in 2010 found that 75% of participating companies reported an increase in employee productivity through the use of mobile applications. This was broken down into: improved employee responsiveness and decision-making (66%); faster resolution of customer and internal IT issues (48%); and improved customer satisfaction (42%)[4]. This indicates that the benefits are there for organisations to take advantage of.

**Protecting information when mobile**

Protection of mobile technology needs to be incorporated with the overall security strategy and the key is to focus on the information rather than device or location. Mobile users tend to have lower security awareness than a PC user, as smartphones have more built-in security so the risks are, to some extent, lower. However, there are still threats around and they are increasing.

As more smartphones are being used in business, instances of malware are also on the rise. Symantec Internet Security Threat Report research found that Android malware doubled from 2010 to 2012[5]. It is believed that currently, more than half of all Android threats collect device data or track users' activities. It is therefore crucial for bank IT teams to be able to remotely control mobile data, especially if a device is lost or stolen.

**Total Mobile Malware Family Count 2010-2012**




*Source: Symantec Internet Security Threat Report, 2011*

The Symantec State of Mobility 2012 survey showed that organisations rate mobility highest among IT initiatives in risk[6]. They're worried about losing devices, data loss and malware infecting the corporate network through smartphones and tablets.

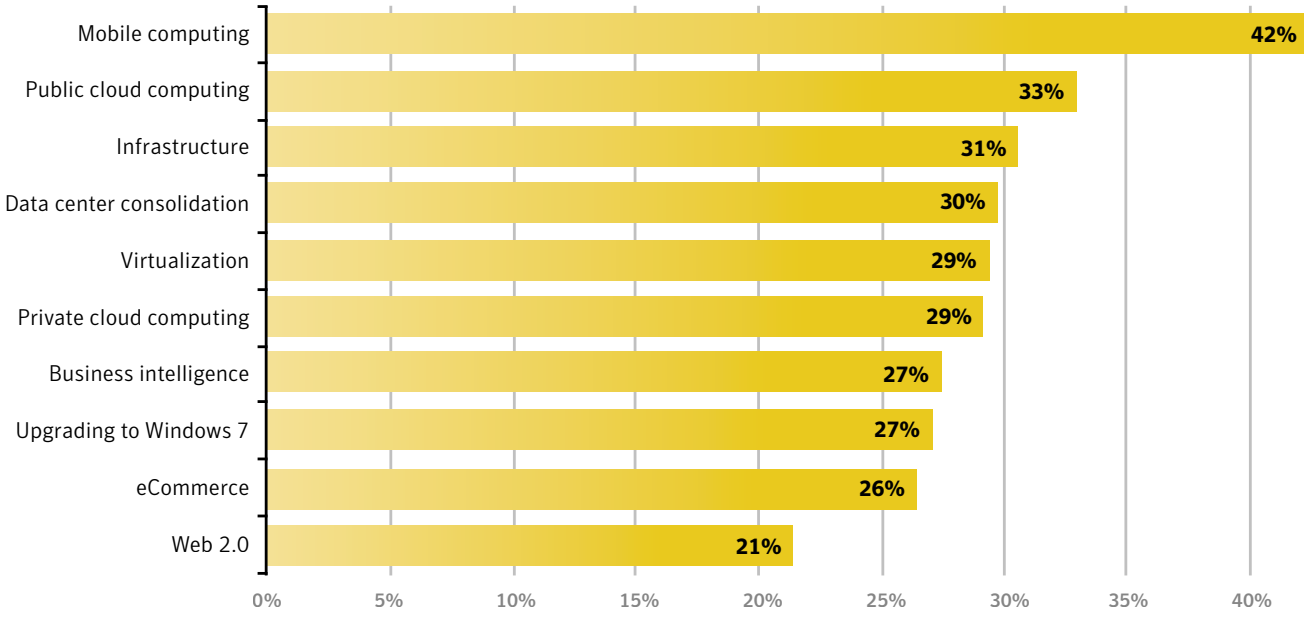
There are good reasons for these concerns. Globally, businesses are losing a significant amount of money to incidents relating to mobile devices – as much as USD $429,000 annually in the case of large enterprises.

Despite these losses, organisations feel the risks are worth the benefits, and they are working to implement security measures to rein in costs and protect corporate information.

Safeguarding customer information makes the challenge even greater. Mobile computing represents a particular risk to identity and access management. In addition, customer maturity levels and security awareness also need to be taken into consideration and this varies between countries. In the Nordics, awareness and protection is high, while Southern and Eastern Europe countries have little security in place. Adding partners into the scenario also increases the complexity of the challenge.

However, it is important to remember that the largest security threat comes from employee behaviour. Internal controls are vital, particularly relating to issues such as data loss prevention and compliance.

**What are the top three computing initiative risks in terms of the level of risk they introduce for your organisation (in the top 3)?**




*Source: Symantec State of Mobility Survey, June 2012*

## Leveraging the cloud

The proliferation of mobile devices at home and in business has been largely fuelled by the growth in cloud-based services and applications. It adds another dimension to mobile, as services hosted in the cloud are accessible through mobile devices. It is beneficial to users as information is available from a single source, simplifying collaboration and control. Banks have traditionally been slow to adopt cloud services, but mobile usage will drive that need if organisations are to leverage the full capabilities of the technology.

Cloud services can offer agility, cost efficiency and predictability, and can extend the capabilities of mobile technology. However, cloud computing is not without risks, including unmanaged employee use of cloud services such as file sharing websites or participation in social networking sites. Ironically, the tighter the IT department holds the reins, the more likely it is that employees will work around limitations using third-party websites or applications.

**The main risks involved in the use of ad-hoc cloud computing services include:**

- Security and compliance – the interfaces between users, endpoints and backend systems all need to be secure with appropriate levels of access control in place.
- The need to encrypt data as it is transferred over the Internet.
- The danger of non-compliance with data protection regulations – for example, if the data is hosted overseas, from a European standpoint this could result in a breach of privacy legislation.
- Lack of vendor validation – is the service reputable and secure? Can the users easily transfer their data to another vendor should the need arise?
- The need for strong service level agreements (SLAs) to promote high system availability.
- Secure access control over company data stored on third party systems. Does the service offer control over how the data is stored and how it can be accessed?
- Inability to access own data if the service is unavailable for any reason.
- Legal risks and liabilities that may arise as a result of vendor terms and conditions. The terms and conditions need to be clear and service level performance monitored against the agreed SLAs.

Despite these risks, businesses are embracing the benefits of cloud computing and mobile working, and the price and performance advantages of consumer devices to reduce costs and improve productivity. According to Symantec research in 2011, 37% of businesses globally are already adopting cloud solutions[5].

The risks of unmanaged employee adoption of cloud computing or the use of consumer devices and consumer websites in business are clear. But even if companies deliberately choose consumerisation, there are still security challenges. Cloud computing makes it harder for companies to erect an impermeable boundary around the business and track and control how data is stored, managed, transferred and used.

IT managers and CISOs can address these concerns by validating an approved list of cloud applications. This needs to be backed-up with the appropriate acceptable usage policies, employee training and, if necessary, enforcement using website access control technology. In addition, when employees access consumer sites for business use, companies need to protect users against potential attacks from Web-hosted malware and spam.

## Using mobility to gain a competitive edge

Customer adoption of digital technologies keeps growing and will continue to drive long-term shifts in customers' financial behaviour and the way banking products are distributed.

**Say yes to new revenue streams**

To compete with new entrants, traditional banks need to find ways to add value for customers and increase revenue. This brings security and compliance challenges at a time when authorities are continuously raising the bar and margins are shrinking.

The key is to act before the majority of your users do:

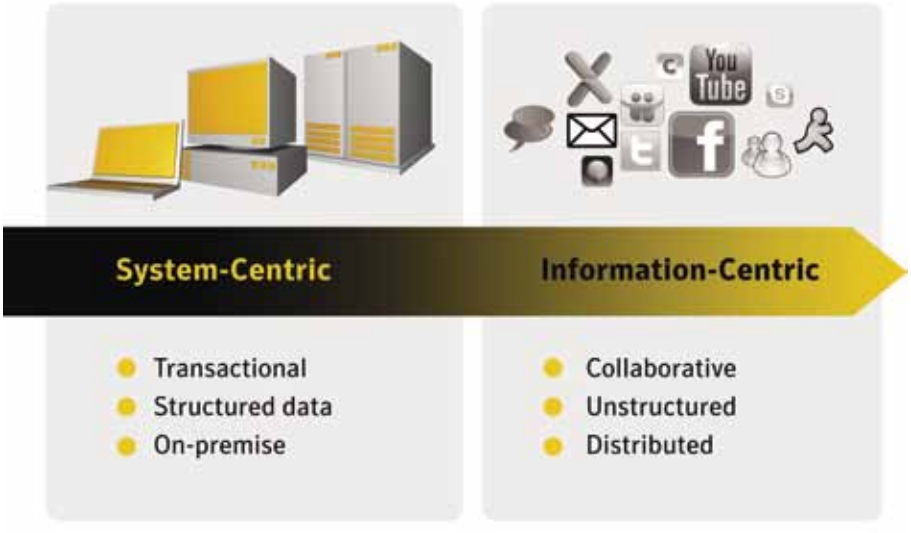
- Set up automated controls that monitor behaviours and talk to customers or employees in order to anticipate needs or issues.
- Say yes to bring your own device, but make sure management is in place for the device, the application or the related information.
- Ensure there is an overarching mobile strategy defining the objectives, restrictions and responsibilities and policies are enforced accordingly.

Mobile provides a new route to market and an additional channel for customer engagement. The true challenge of the CISO will be to balance this innovation with the increase in risk.

**Create a transparent business and IT risk view**

Governance and risk management are fundamental when embracing mobile. The information must be readily available and communicated to executive management as a decision criterion for investments and projects (that are crucial for the business objectives). The emphasis should be an information-centric approach, where risk and compliance need to be upheld regardless of device or location.

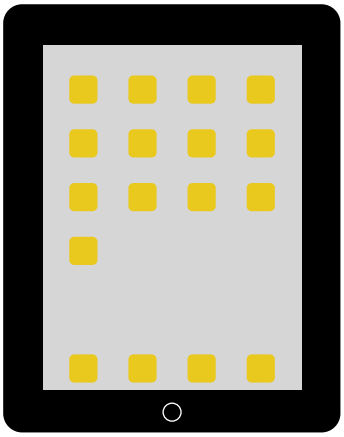
Symantec research revealed that information volume is expected to grow 67 percent over the next year for enterprises[5], so automation will be vital.



**Protect employees and customers**

Mobile security and device management are the foundations of an enterprise mobility strategy. There are multiple choices of level of management for devices, as well as the option to focus instead on securing applications and information.

Organisations should consider all mobile worker types and functions before deploying solutions. Banks need to consider solutions across the security sub-segments that secure endpoints, provide protection for the corporate network, and protect data as it moves over wireless or mobile networks. End user education and buy-in are central to a successful, secure enterprise mobility roll out.



For customers and partners, security requirements can be added for accessing applications and networks. Another viable option is to offer security solutions, tools or training at a reduced price, in order to minimise external impact on the bank's network and data. Availability is crucial as users expect 24/7 access to services.

With BYOD and cloud, information is no longer within the four walls of a company. Protection must focus on the information, not the device or data center.

**Build trust and competitive positioning**

A second-generation mobile strategy will expand beyond IT (business-to-employee [B2E]) and marketing (business-to-consumer [B2C] or B2B). It will include a much broader set of decision makers, funding sources and partners. New approaches to governance, as well as increased risk assessment and mitigation strategies, will be required.

As competition increases and the number of mobile players in the banking ecosystem is multiplying, traditional and trusted financial institutions can build on their solid position to expand. Creating niche players and even additional brands will be necessary from time to time, so online and traditional channels can exist side by side.

**Increase productivity through the workplace**

Employee satisfaction is an important measure for success. The constant need to raise productivity will result in increasing numbers of banks embracing mobile working for employees. As a result, branches can offer more rapid service to customers, employees can be online regardless of location, and executives and management can easily collaborate to share business information.

Productivity gain should be a critical measure of success in an enterprise mobility strategy to ensure that investments fulfil their purpose. Even though positioning and PR are attractive and desired, the business impact that mobile can deliver will be measurable and visible to the organisation.

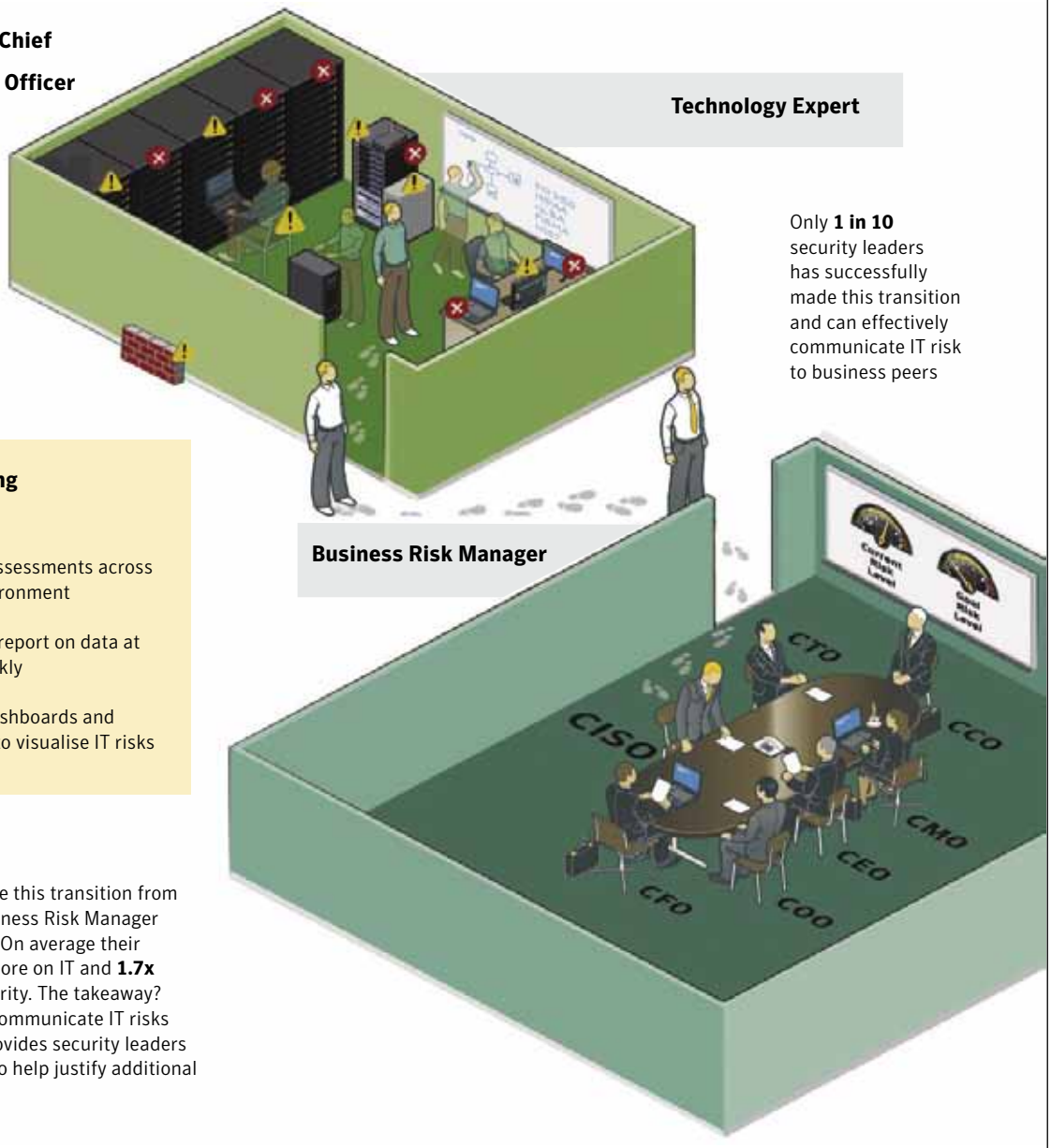
**Balancing risk with opportunity**

Risk management is at the core of mobile and banking. As transaction volumes increase, maintaining service quality will necessitate a move from manual to automated processes. To achieve competitive advantage, risk management tools need to be up-to-date and readily available. Balancing risk with opportunity is the daily challenge of the CISO and greater transparency will be needed so that business decisions can be taken faster and on firmer grounds.

## From Chief Information Security Officer to Business Risk Officer

As security and risk management is moving closer to the boardroom, the job of the Chief Information Security Officer is changing. Risk management is becoming more central as the demand for business-driven IT is increasing alongside pressure to reduce costs, leverage new services and become more agile as competition grows. **The role of the CISO** is changing and mobile has been a strong driver as it derives directly from the users, making it a faster movement and demanding other tools and methods to manage risk.

**Changing role of the Chief Information Security Officer**




Only **1 in 10** security leaders has successfully made this transition and can effectively communicate IT risk to business peers

**What are they doing differently?**

**69%** Automate assessments across their IT environment

**61%** Collect and report on data at least bi-weekly

**75%** Leverage dashboards and scorecards to visualise IT risks

### A valuable transition

Security leaders who make this transition from Technology Expert to Business Risk Manager also secure more budget. On average their organisations spend **3x** more on IT and **1.7x** more on information security. The takeaway? Being able to effectively communicate IT risks in business terms also provides security leaders with the metrics needed to help justify additional security investments.

## Conclusion

Banks need to focus on new technologies as they shift from a branch-centric culture to a digital-centric strategy that is focused on earning loyalty by delivering great customer experiences across multiple touchpoints. To stay competitive, banks need to provide enterprise mobility solutions that embrace employee needs, automate and refine risk management, implement future-proof solutions and invest in mobile customer services to achieve competitive advantage and customer satisfaction.

Banks investing in mobility and security now will be better positioned to gain competitive advantage and strengthen their role as a trusted party.

## The right partner for a mobile world

Symantec protects information for banks, their employees and their customers. Symantec is a global leader in providing security, storage and systems management solutions to help customers – from consumers and small businesses to the largest global organisations – secure and manage their information and identities independent of device. Symantec brings together leading software and cloud solutions that work seamlessly across multiple platforms, giving customers the freedom to use the devices of their choice and to access, store and transmit information anytime, anywhere.

## References

1 IDC Worldwide Smartphone 2012-2016 Forecast Update: June 2012, doc #235193
2 Gartner Forecast - Mobile Data Traffic and Revenue, Worldwide, 2010-2015 July 2011 - Doc ID:G00213763
3 IDC Social Business Survey, 2011
4 Forrester Enterprise And SMB Networks And Telecommunications Survey, North America And Europe, Q1 2010
5 Symantec Internet Security Threat Report, 2011
6 Symantec State of Mobility Survey, June 2012

**Further reading**

BYOD whitepaper: Exploiting the business potential
**https://www4.symantec.com/Vrt/offer?a_id=138354**

**Glossary**

- BYOD (Bring Your Own Device)
- IAM (Identity and Access Management)
- First platform: Mainframe/Terminal
- Second platform: Client Server/PC
- Third platform: Mobile/Cloud

**Author**

Marie Pettersson - Symantec Corporation

## Notes

## Notes

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organisations secure and manage their information-driven world with data deduplication and deployment software.