HKU920

Asia Case Research Centre
THE UNIVERSITY OF HONG KONG

POON
Poon Kam Kai Series

INDRANIL BOSE

HDFC BANK: SECURING ONLINE BANKING

As we get down to reinforcing our information security defences at HDFC Bank, I am grappling with three major dilemmas. How do I ensure the security of an online transaction while still keeping customer convenience as a priority? Should I make secure access mandatory or should I leave it discretionary? Should I go for an onsite model or for the cloud model?

- Vishal Salvi, chief information security officer, HDFC Bank[1]

In August 2007, HDCF Bank—one of India's leading private banks, with deposits of Rs 682 billion (US$15.64 billion)[2] [see **Exhibit 1**]—was the target of a phishing attack. Customers were receiving e-mails claiming to have originated from the bank and seeking sensitive account information, including passwords and personal identification codes.

At the time of the attack, 1.28 million customers, amounting to 28% of the HDCF Bank's retail customers, were banking online. Online security provided to these customers consisted of the use of a user ID and password to gain access to the payment gateway, a level of security referred to in banking circles as "first level" security. As the chief information security officer, Vishal Salvi had been working on strengthening the bank's information security ("IS") framework. The phishing attack had brought a new sense of urgency to the task before him.

The Indian Banking Industry

The Indian banking industry consisted of five types of banks: public sector banks ("PSBs"), which were owned by the federal government; private sector banks; co-operative banks; regional rural banks; and foreign banks. The industry was regulated by the country's central bank, the Reserve Bank of India (RBI). There were 28 PSBs, 27 private sector banks, 55 urban co-operative banks, 133 regional rural banks, and 29 foreign banks as of March 2006.[3]

[1] Company interview conducted on 16 September 2010.
[2] US$1 = Rs 43.59 on 30 March 2007.
[3] RBI (2010) "Banking Statistics", http://rbidocs.rbi.org.in/rdocs/Publications/PDFs/78903.pdf (accessed 26 September 2010).

R. Chandrasekhar prepared this case under the supervision of Dr Indranil Bose for class discussion. This case is not intended to show effective or ineffective handling of decision or business processes.

Ref. 10/479C

The federal government had launched a series of banking reforms in 1994, including deregulation of interest rates, infusion of new capital for PSBs, consolidation of banks through mergers and acquisitions, provisions for new banks to be set up in order to promote competition, and reinforcement of the regulatory framework. The reforms had a major impact on the overall efficiency and stability of the banking system in India.[4]

The operations of PSBs were largely branch-based. Customer interactions were limited to banking hours and took place only over the counters. Although they had built up high levels of trust with their customers, PSBs were burdened with legacy systems and processes resulting in slow response times. In contrast, new-generation private sector banks, such as HDFC Bank, were able to provide 24/7 service to customers by deploying self-service channels such as phone banking and ATMs right from day one. As of March 2007, 78% of customer-initiated transactions at HDFC Bank were serviced through non-branch channels, including ATMs, phone banking, internet banking and mobile banking.[5]

In March 2004, the RBI had made it mandatory for all banks to route their high-value payments (in excess of Rs 100,000) through the real-time gross settlement system ("RTGS"). As a result, electronic payments were overtaking paper-based payments in terms of value. By March 2007, RTGS accounted for 96% of the value of payments, but comprised only 1% of banking transactions by volume.

IS in the Banking Industry

The internet made its debut in India in August 1995 when Videsh Sanchar Nigam Ltd (VSNL), a telecom enterprise owned by the federal government, launched dial-up facilities in six Indian cities. Worldwide, the total number of internet users stood at 16 million at the time. By January 2010, the number had reached 1.65 billion [see **Exhibit 2**].

India had a total of 2.52 million internet subscribers as of March 2007 [see **Exhibit 3**]. Of these, 2.4 million were broadband subscribers (with download speeds of 256 kbps or more).[6] From the point of view of IS, however, it was the number of internet users that was important for a bank. Because a single internet subscription could provide access for multiple users, the number of internet users was much higher. According to estimates made by the Internet and Mobile Association of India ("IAMAI"), there were 38.5 million internet users in India in 2006. Their numbers were expected to increase to 100 million by 2008.[7]

> *The issue of security in an online banking transaction has five components. The first is authentication. The transaction must ensure clear identity of the person. The second is authorization. The person doing the transaction, at both ends, must be authorized to do so. The third is privacy. The data relating to the transaction must be between the two persons doing the deal and no outsider should gain access to it. The fourth is integrity. The data which is part of the deal must not be altered. The fifth is non-repudiation. A party to the deal cannot deny that it originated the communication or data. A typical IT security system must factor in all the five of them.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

[4] Reddy, Y.V. (2005) "Banking Sector Reform in India—An Overview", *BIS Review*, http://www.bis.org/review/r050519b.pdf (accessed 26 September 2010).
[5] HDFC Bank (2007) "Directors Report of the Annual Report of HDFC Bank", http://www.hdfcbank.com/common/pdf/corporate/Directors_Report0607.pdf (accessed 20 October 2010).
[6] Telecom Regulatory Authority of India (2007) "Annual Report".
[7] IAMAI (2006) "IAMAI's Report Online Banking 2006", http://www.iamai.in (accessed 20 October 2010).

There were two reasons why the banking industry, unlike other industries, was fundamentally compatible with the demands of IS. First, banks were, by the very nature of their business, focused on risk management. Attuned already to the identification, measurement and monitoring of credit risk, market risk and operational risk, they could, with some training, learn to cope with the newly emerging IS risks. Second, every established bank had enjoyed, over the decades, the image of a solid, reliable institution that customers could count on. The banks had a natural advantage in generating and sustaining trust, which was an important element of the relationship—whether online or offline—between a bank and its customer.

This level of trust also partially explained why US banks such as Citibank and Bank of America could easily build up impressive numbers of online clients while pure-play online banks which had no branch network, such as Telebank and NetBank, had difficulty notching up even their first 100,000 online accounts. This was in stark contrast to the situation in other industries such as travel, where incumbent players rose to defend their turf only after internet pure-plays had first mobilised customers online.[8]

The benefits of moving their customers from offline banking to online banking were considerable for banks. It speeded up response times, improved the quality of service and lowered transaction costs. Online banking was beneficial for customers, too, because it gave them flexibility. They could do banking transactions anytime, anywhere, and could take charge and feel empowered. The major stepping stone was security, which was the greatest source of the apprehension customers had about online transactions.

The banking environment in India was competitive. Every bank sought new customers, new deposits and new business. But retail customers generally did not switch their accounts. This was, however, only true of offline banking. Online banking, which was of recent vintage, was opening up avenues for mobility of customer accounts. The level of satisfaction with online experiences was a major factor influencing the decision to switch to online accounts.

RBI Regulations

In June 2001, the RBI issued a set of guidelines regarding internet banking.[9] The guidelines stipulated that the security policy of a bank should be approved by its board of directors. The bank should introduce access controls for data, systems, application software, utilities, libraries, system software and telecommunication lines through such tools as user IDs, passwords, smart cards and biometrics. It should use a proxy-server-type firewall so that there would be no direct connection between the user and the bank's system. The RBI recommended that the application server be isolated from the e-mail server and that all computer accesses be logged. It favoured Public Key Infrastructure ("PKI") as the technology for securing internet banking services.

The RBI guidelines also stipulated that a bank review its security infrastructure and security policies regularly in light of both its own experiences and changing technologies. The information security officer and the information system auditor should undertake periodic penetration tests of the system. The tests would include such tasks as deploying password-cracking tools, searching for back-door traps in the programs, checking for commonly known holes in the software (especially the browser and e-mail software), engaging outside experts (often called "ethical hackers") to infiltrate the system, testing physical access controls, inspecting the infrastructure and schedules for backing up data, and conducting mock disasters to test data recovery and ensure business continuity.

[8] Boss, S., McGranahan, D. and Mehta, A. (2000) "Will the Banks Control On-Line Banking?", *McKinsey Quarterly*, www.mckinseyquarterly.com (accessed 25 January 2010).
[9] RBI (14 June 2001) "Internet Banking in India—Guidelines", http://www.rbi.org.in/notifications (accessed 12 February 2010).

Banks were also required to conduct risk management analyses and security vulnerability assessments at least once per year, and to maintain full, up-to-date documentation of security practices, guidelines, methods and procedures used in mobile banking and payment systems. They were also required to implement physical security measures to protect system gateways, network equipment, servers, host computers, and other hardware and software from unauthorised access and tampering. Data centres were to incorporate proper network protection mechanisms. Banks were also required to ensure that the internet banking login IDs and passwords of each customer would be different from those used for mobile banking.

In November 2006, the RBI also released guidelines on outsourcing of financial services by banks, and was in the process of preparing a separate set of guidelines for mobile banking. RBI regulations were considered prescriptive only as far as basic controls were concerned. For example, in the area of outsourcing, the RBI was categorical in requiring that IS vendors not store confidential information at their end and that all customer-centric information be encrypted. However, the RBI did allow banks to choose their own individual authentication systems.

Online Customers

Online banking was in its early stages in India. Customers would log on to their online accounts for information (e.g., account history and balance) and communication (e.g., to receive alerts from the bank and send messages to the bank). It was only when the medium was used to conduct financial transactions, such as transferring funds and paying bills, that the adoption of the medium would be complete. The trend towards the transactional stage was being driven by the participation of young professionals across the country. Those above 35 years of age were generally used to visiting the bank in person each month to deposit their salary cheques and withdraw money over the counter. The physical presence of a bank and the personal interaction with the staff were greater sources of trust for them than the secure controls provided in online banking.

A survey conducted by IAMAI in December 2005 with a sample size of 6,365 respondents provided some insight into the profile of online banking customers in India. The survey was conducted online and cut across age, gender, education and occupation.

According to the survey, 43% of the users of online banking were in the age group 26–35, and 25% were in the age group 18–25. The demographic consisted in large part of young, internet savvy professionals. Of all online baking users, 83% were male, 85% had a university degree, and 57% were in executive positions. A majority of them owned plastic cards—86% had ATM cards, 65% had credit cards and 78% had debit cards—pointing to their trust in a cashless medium. Of users of online banking, 64% accessed the internet from their homes and 73% from their offices. For purposes of online banking transactions, 41% accessed their online accounts from home and 48% from their offices. As an indicator that the internet had become an integral part of their daily activities, 88% used the internet for more than 5 hours per week.[10]

HDFC Bank Background

As one of the first new-generation private sector banks to come into being as a result of banking liberalisation measures initiated by the federal government of India in 1994, HDFC Bank commenced operations in January 1995. It was promoted by HDFC, a premier housing finance company that had developed a core competence in retail mortgage loans. HDFC Bank

[10] IAMAI (2006) "IAMAI's Report Online Banking 2006", http://www.iamai.in (accessed 20 October 2010).

started offering online banking services soon after the RBI published its guidelines on internet banking in June 2001.

Headquartered in Mumbai, HDFC Bank had an income of Rs 84.1 billion (US$1.93 billion) for the year ending March 2007 and a profit before tax of Rs 11.4 billion (US$260 million) [see **Exhibit 4**]. The bank had a total of 10 million customers as of March 2007, of whom savings account holders were the single-largest category, comprising 4.6 million customers. A total of 21,477 employees served these customers through a network of 684 branches and 1,605 ATMs in 316 cities across India.[11]

HDFC Bank had three business segments: retail banking (offering financial products and banking services to individual customers); wholesale banking (providing commercial and transactional banking products to corporate clients); and treasury (consisting of foreign exchange and derivatives, local currency money market and debt securities, and equities).

As a recent entrant in the Indian banking sector, HDFC Bank had no legacy or baggage to cope with. It could invest in the latest hardware and software solutions in order to "deliver operating value and leverage, and enrich customer experience"[12]. It operated in a highly automated information technology environment, and all the bank's branches were linked to one another online.

The bank was focussed on semi-urban and under-banked markets, with 64% of its branches located outside the top nine Indian cities. Its goal was to be "the preferred provider of financial services to upper- and middle-income individuals and leading corporations in India".[13]

> *HDFC Bank has identified its mission as becoming "a world class Indian bank." It has defined its business strategy as comprising the following elements: Increase the market share by balancing quality and volume growth; Leverage technology to deliver more products to more customers and to control operating costs; Maintain asset quality through disciplined credit risk management; Develop innovative products and services that attract targeted customers, reduce the cost of funds and address inefficiencies in the Indian financial sector; and. finally, Focus on healthy earnings growth with low volatility.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

The internal risk management models used by HDFC Bank were technology-intensive. For online transactions, the bank used what was known as "adaptive risk modelling", wherein the operating system assigned a risk score to each transaction on the basis of pre-determined parameters (such as the pattern of use, size of transaction and geographical location); the higher the risk score, the greater the level of intervention by the system. The intervention would vary from asking the customer to use a one-time password, calling up the customer to verify the transaction or blocking the transaction automatically.

Customers could log in to their online accounts with a user ID and password and check their balances, view their transaction history, and transfer funds between their own accounts and to

[11] HDFC Bank (20 July 2007) "Form 20-F", United States Securities and Exchange Commission, http://www.sec.gov/Archives/edgar/data/1144967/000119312507152669/d20f.htm#rom97808_4 (accessed 5 July 2010).
[12] Srikant_Srinivas, "Faster, Safer, Larger Banking," http://www.businessworld.in/December 19, 2009 (accessed 5 July, 2010)
[13] HDFC Bank (18 July 2007) "Form 6-K," United States Securities and Exchange Commission, http://www.sec.gov/Archives/edgar/data/1144967/000119312507157033/0001193125-07-157033.txt (accessed November 30, 2010)

any other HDFC Bank account. They could also open a fixed deposit, make a stop-cheque request and view the status of a cheque online.

The bank's centralised data centre and back-up systems were located at two separate sites in Mumbai. The bank also had a remote disaster recovery site in Bangalore that could replicate its network in the event of a natural disaster at the main sites.

Mobile Banking

As chief information security officer, Salvi's principal mandate was to make certain that HDFC Bank's online banking platform was secure from online hazards. Online banking had two components: net banking and mobile banking. The latter was still a new concept in India but was widely considered to be the banking medium of the future.

Mobile banking was gaining ground worldwide. A forecast by Frost & Sullivan had placed the world mobile penetration at over 50% of the population by 2015 [see **Exhibit 5**]. In India, the number of mobile subscribers had grown steadily from 60.85 million in 2005–2006 to 98.77 million subscribers in 2006–2007 to 165.11 million for the year ending March 2008.[14] Over time, users of mobile phones would likely be conducting banking transactions on their mobile phones. Ensuring a secure mobile banking platform was thus an integral part of the strengthening of online banking at HDFC Bank.

> *There has been a gradual change in the ecosystem of banks in India as each bank transitions from the brick and mortar model towards the click and portal model. One aspect of this change is the growing inter-dependence between banking and telecommunications sectors. For us at HDFC Bank, an IS framework, in the light of the changing ecosystem, has three dimensions - technology integration, business integration and risk integration.*
>
> *A major aspect of technology integration is that IS should be independent of the larger information technology (IT) scenario at the bank. A major aspect of business integration is that each business division in the bank should be accountable for the costs and risks associated with IS. A major aspect of risk integration is that each employee should look at IS risks as part of overall risk management of the bank rather than as a standalone risk. At HDFC Bank, we are today at the beginning of the curve in each of these areas.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

Dilemmas in Strengthening Security

Phishing was one of the nine most common online frauds concerning the banks and financial institutions of the developed world [see **Exhibits 6** and **7**]. One out of every 115 customers in the US had lost money in 2006 due to phishing, averaging $850 per incident. The total damage to the US economy due to phishing amounted to $630 million in the single year 2006[15] [see **Exhibit 8**], and phishing attacks were on the rise worldwide [see **Exhibit 9**].

Phishing had first become evident in Indian banking in late 2006, and HDFC Bank was the fourth Indian bank to encounter it. Indian banks had long been immune to phishing because online banking had not reached a critical mass in the country. When the phishing attack on its

[14] Telecom Regulatory Authority of India (2008) "Annual Report".
[15] Consumer Reports (September 2006) "State of the Net", www.consumerreports.org (accessed 2 September 2010).

customers first came to light in August 2007, HDFC Bank was quick to take corrective measures.

It signed on with RSA Security, a US-based provider of IS solutions with whom it had been in talks for a while, to set up a 24/7 command centre. RSA Security, in turn, deployed its E-Fraud Action suite, which it had developed for the banking sector. The suite would enable RSA Security, as the service provider, not only to monitor an ongoing phishing attack but to shut down, under authorisation from HDFC Bank, the bank's online transactions temporarily, leaving only the option of transactions over the counter available to customers.

The bank also introduced a "cooling period" wherein transfer of funds to a new person not listed by the account holder as a beneficiary would take effect only after 24 hours. This would give time for the bank to check the transaction and also for the account holder to alert the bank. The bank also began sending awareness messages to customers in an effort to educate them about the hazard of phishing.

One of the goalposts for Salvi in his role as chief information security officer was to ensure that the IS protocols were not so rigorous as to cause inconvenience to customers. Although HDFC Bank was not pursuing market share as a business objective in its own right, securing regular annual increases in new customer accounts was crucial to business growth, and ensuring that existing customers stayed on with the bank was equally important.

Customer Convenience

Salvi had to strike a balance between keeping the IS transparent to the customer (so that he or she breezed through an online transaction without barriers) and making it effective from the bank's point of view (so that the bank was not taken for a ride by potential fraudsters). Putting in place processes that would track the loose ends of an individual transaction and tighten them up was important. But it was equally important not to undermine the overall level of trust customers placed in the bank.

Every online transaction, irrespective of such variables as the size of the transaction, would have to go through standard checks. The checks would use a combination of validation (i.e., "what the customer knows") and authentication (i.e., "what the customer has"). Each transaction had to have proper validation in terms of a user ID and password, both of which were known only to the account holder. The transaction also required proper authentication, which could be in the form of a token, which was a physical device that was battery-powered and provided a dynamically generated six-digit number that would vary with each transaction. Validation and authentication were the minimum requirements for approving an online financial transaction, however small.

There were also additional check points, depending upon the profile of the customer, that the IS system was programmed to generate on the basis of the historical footprints of the account holder. Any transactional behaviour that was not in conformity with the profile would raise a red flag, alerting the IS system. Some examples were the number of transactions in excess of a typical transaction in the customer account, the account being activated at a location different from where the customer would normally initiate an online transaction, and the account being accessed from an IP address different from the one normally associated with the account.

According to Salvi, the security check at an airport was an instructive parallel. An airline passenger wants to go through the drill quickly and move on, but the security personnel are in no such hurry. They are focused on a different objective of preventing a mishap in the aircraft.

They therefore put every customer, without exception, through mandatory checks such as frisking and verifying ID. They also isolate some, based on random selection or individual perceptions, for additional checks. The selections are statistically sound and perceptions are invariably rooted in valid grounds but, in the final analysis, not all additional checks are warranted.

> *In the online world, we call it "false positive rate." If the IS protocol identifies a financial transaction as suspect and the transaction turns out to be genuine, it would be a false alarm. It is a performance metric we track regularly. While it will be our endeavour, as a bank, to reduce the false positive rate, the rate will come down only as the IS technologies mature and the IS processes are stabilized. That takes time. But customers perceive it as an inconvenience. It is a perception that affects a bank's competitive positioning.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

The major predicament Salvi was facing in the context of customer convenience was whether the IS protocols being installed at HDFC Bank should authenticate the identity of the account holder or whether they should authenticate the transaction. Authentication of identity concentrated on the account holder as an individual and required the use of authentication instruments such as biometrics (which focused on "what you are" as an electronic persona) and tokens (which focused on "what you have" as an account holder). Authentication of transactions concentrated on the integrity of the transaction as a process. It required the use of risk-scoring instruments such as the amount being within the range of an account holder's average transaction and the recipient being a beneficiary designated by the account holder.

Each was a new layer and each new layer added to the complexity of the process. Customers, on the other hand, were seeking simplicity; but they also wanted the system to be trustworthy, a factor that was taken for granted in offline banking.

Secure Access

A majority of HDFC Bank's online customers were using the internet at least once a month, but there were also dormant users, amounting to approximately 20% of registered online customers. They would almost never use the internet, even though they had registered for online banking, and would instead use offline media such as ATMs or visit a branch in person.

Salvi was planning to introduce a second level of authentication for all online customers as part of ensuring what was known in banking circles as "secure access". It would incorporate details of authentication that were specific to individual customers, such as an image (chosen from among several categories provided by the bank), a personal message, the customer's address or telephone number, and answers to any of five different questions (which would be asked at random by the IS system during an online transaction). The details would be part of the process of validation of the account holder by the system, which had no provision for intervention by bank personnel at the time of a financial transaction.

Another major part of secure access was asking the customer to provide the bank with a list of account holders, known as "beneficiaries", with whom the online customer's transactions would be periodical and regular.

Dormant accounts were a common phenomenon in offline banking, where they posed no particular hazard to the bank, on the principle of "no usage, no fraud". In an online

environment, however, this principle did not hold. Dormant accounts were vulnerable to attacks because a fraudster could gain entry through them without raising an alert.

The issue before Salvi was whether the bank should provide secure access to every registered online user or limit secure access only to active users. It was important to provide a timeframe for dormant users to seek secure access before disabling their accounts, but the window had to be small to prevent misuse during the interim period.

> *We have the dilemma only with regard to existing online customers. For new customers, hereafter, seeking online registration, we will provide Secure Access simultaneously. We will also automatically disable the access for customers who will not use the online medium regularly. Once disabled, they will have to visit a branch in person with an ID to gain Secure Access once again. The process will be mechanical. But with existing online customers who are dormant, we have an issue about how long we should retain them in the system unguarded, before disabling them. A fraudster can steal an ID and password of dormant online customer, make a false registration, set up himself as a beneficiary and transfer funds during the unguarded, interim period. It is a ticking time bomb.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

Server Location

The proposed IS infrastructure at HDFC Bank would include two types of servers: authentication servers (housing the software that would conduct the due diligence) and online servers (facilitating the actual transfer of money from one account to another). The dilemma before Salvi was whether the servers should be located onsite, at HDFC's own data centres in India, or whether they should be offsite, hosted by an IS vendor for a fee. The bank was in talks with RSA Security, already involved in countering the phishing attack, as a likely vendor.

An onsite model carried a low rate of systemic failure because the servers would be an integral part of HDFC's own local area network. An offsite model required a separate medium of communication between HDFC Bank and the IS vendor—the internet—and keeping this medium secure on an ongoing basis would be yet another of the potential tipping points. A related dilemma was whether the online servers should be located at HDFC's data centres and the authentication servers at RSA's premises. The latter were outside of India, which, in the light of transcontinental links not always being robust, would present yet another potential point of systemic failure.

RSA Security had built up a competence in cloud computing, which was the most recent development in the evolution of offsite models. The "cloud" was a term that denoted the sum total of users' resources which were stored in the virtual world (i.e., the internet), rather than in the physical world (such as the servers at a bank's data centre). The main advantage of the cloud, as its name suggested, was that it was fluid and elastic. It could expand and contract depending upon the need of the user to scale up or scale down the relevant computing services. This was unlike the fixed capacity of a data centre, which was idle and not scalable.

Cloud computing had several components, including storage, database, integration, testing and infrastructure. A vendor might offer components individually, such as storage as an independent service [see **Exhibit 10**], or provide a bundle of services as a package.[16] RSA

[16] Linthicum, D.S. (2010) *Cloud Computing and SOA Convergence in Your Enterprise: A Step by Step Guide*, USA: Addison-Wesley, p. 38.

Security offered to store the hardware, software, networks, services, and interfaces of HDFC Bank in the virtual world.

In addition to fundamental issues of IS, Salvi had to consider the time and cost factors, which were equally pressing. The cloud model offered by RSA Security could go live in about nine months, by mid-2008. An online model would take longer (an additional six months) to be put into commission. With RSA Security, HDFC Bank could opt for pay-by-use pricing, whereby the bank would be billed only for actual usage, as was typical of the cloud model. The bank could also write off the amount in a financial year as revenue expenditure. With in-house servers, the bank would have to strike a balance between contending with idle capacity for the present and ensuring scalability for the future. In-house servers would also lead to capital expenditure being spread over a longer timeframe.

The cloud model had multiple options for network connectivity. The first option was the internet, which carried no additional costs except that of low reliability. The second was to build dedicated bandwidth, which would be reliable but would also require upfront investment. The third was a proxy server that would be hosted by a vendor and comprise software and hardware architecture installed in bits and pieces on the bank's end.

> *The choice here looks like a no-brainer. But this is a classic dilemma for an IS professional. The purpose of HDFC Bank is to provide financial services to its customers. The role of IS in the bank is to facilitate that purpose. The choice will have to be made in the light of the fact that hardware and software maintenance, upkeep of websites, management of data centres and provision of links at ATMs are not the core activities of the bank.*
>
> - Vishal Salvi, chief information security officer, HDFC Bank

The Way Forward

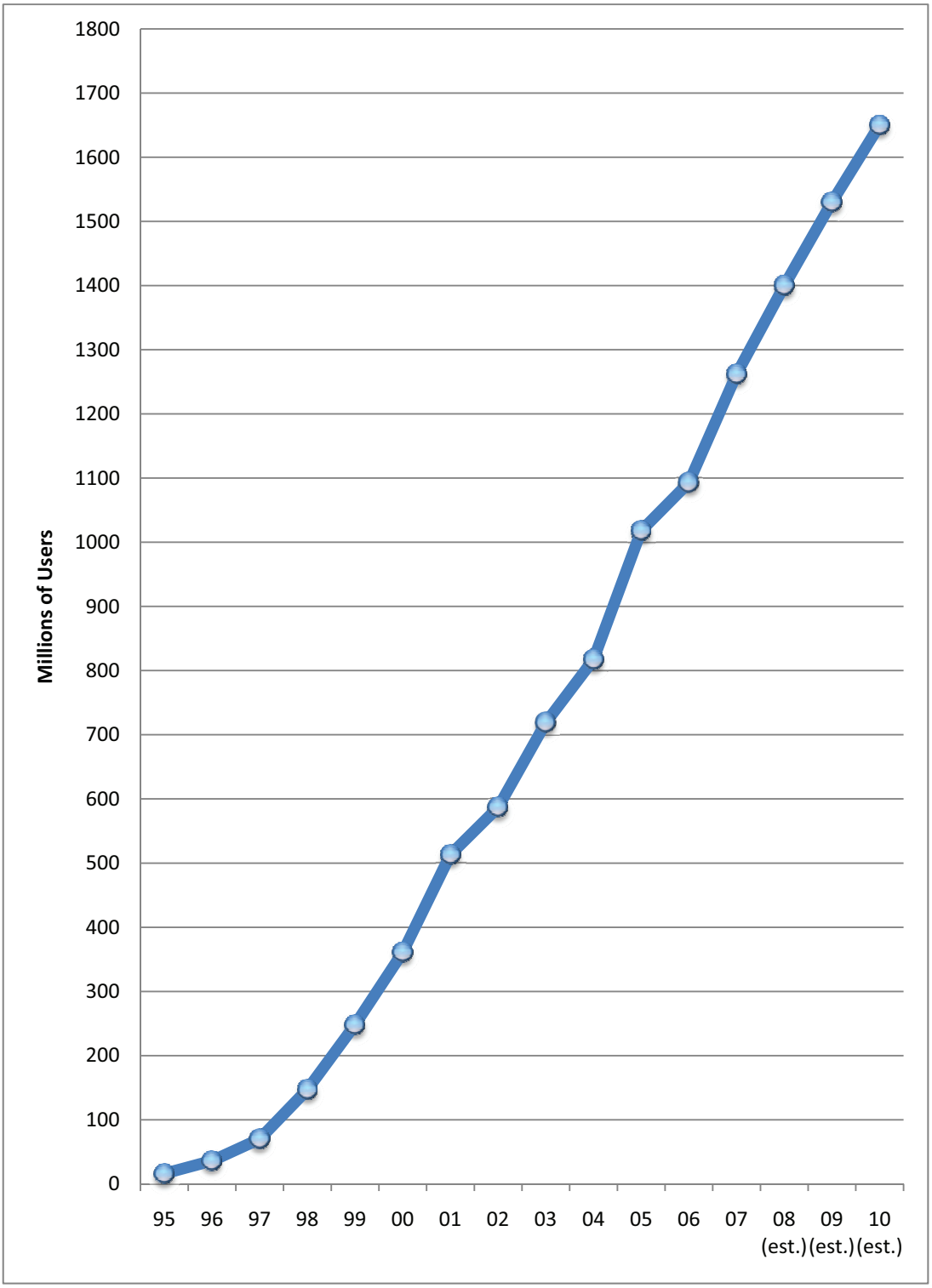
The phishing attacks on banks in India were an indication that the number of online customers of Indian banking had reached a critical mass. Enough online customers had moved enough of their funds online to make an attack worthwhile for a phisher. The challenges of IS would only grow in the future as more and more account holders switched to online banking. Salvi had to establish an IS framework that would make the individual transactions of the online customers of HDFC Bank safe and secure. In doing so, he had to weigh the prospect of installing additional levels of security for each online transaction. There was also the issue of dealing with customers who had registered for online banking but conducted their transactions over the counter. Another issue was whether to continue to host the secure data onsite or take it offsite.

EXHIBIT 1: INDIAN BANKS RANKED BY DEPOSITS, 2007

#	Name of the Bank	Deposits (in billion INR)
1	State Bank of India	4,355
2	ICICI Bank	2,305
3	Canara Bank	1,423
4	Punjab National Bank	1,398
5	Bank of Baroda	1,249
6	Bank of India	1,198
7	Union Bank of India	851
8	Central Bank of India	827
9	Syndicate bank	786
10	Indian Overseas Bank	687
11	HDFC Bank.	682
12	UCO Bank	648
13	Oriental Bank of Commerce	639
14	Allahabad Bank	595
15	Axis Bank	587

Source: Business Today (25 February 2008) "The Best Banks 2007", www.business-today.com (accessed 25 September 2010).

EXHIBIT 2: WORLDWIDE INTERNET USER GROWTH



Source: Internet World Stats: Usage and Population Statistics (January 2008) http://www. internetworldstats.com/stats.htm/January 2008 (accessed 21 October 2010).

EXHIBIT 3: COUNTRY RANKING OF INTERNET SUSCRIBERS, 2007

#	Country	Number of subscribers	Population	Penetration rate
1	US	66,213,257	301,967,681	21.9
2	China	48,500,000	1,317,431,495	3.7
3	Japan	27,152,349	128,646,345	21.1
4	Germany	17,472,000	82,509,367	21.2
5	Korea, South	14,042,728	51,300,989	27.4
6	UK	13,957,111	60,363,602	23.1
7	France	13,677,000	61,350,009	22.3
8	Italy	9,427,300	59,546,696	15.8
9	Canada	7,675,533	43,440,970	23.7
10	Spain	7,505,456	45,003,663	16.7
11	Brazil	6,417,000	186,771,161	3.4
12	Netherlands	5,388,000	16,447,682	32.8
13	Taiwan	4,505,800	23,001,442	19.6
14	Australia	3,939,288	20,984,595	18.8
15	Mexico	3,728,150	106,457,446	3.5
16	Turkey	3,632,700	75,863,600	4.8
17	Russia	2,900,000	143,406,042	2.0
18	Poland	2,640,000	38,109,499	6.9
19	**India**	**2,520,000**	**1,129,667,528**	**0.2**
20	Sweden	2,478,003	9,107,795	27.2
Top 20 countries		268,150,077	3,890,377,607	6.9
Rest of the world		36,121,302	2,684,288,810	1.4
Total world subscribers		304,471,379	6,574,666,417	4.6

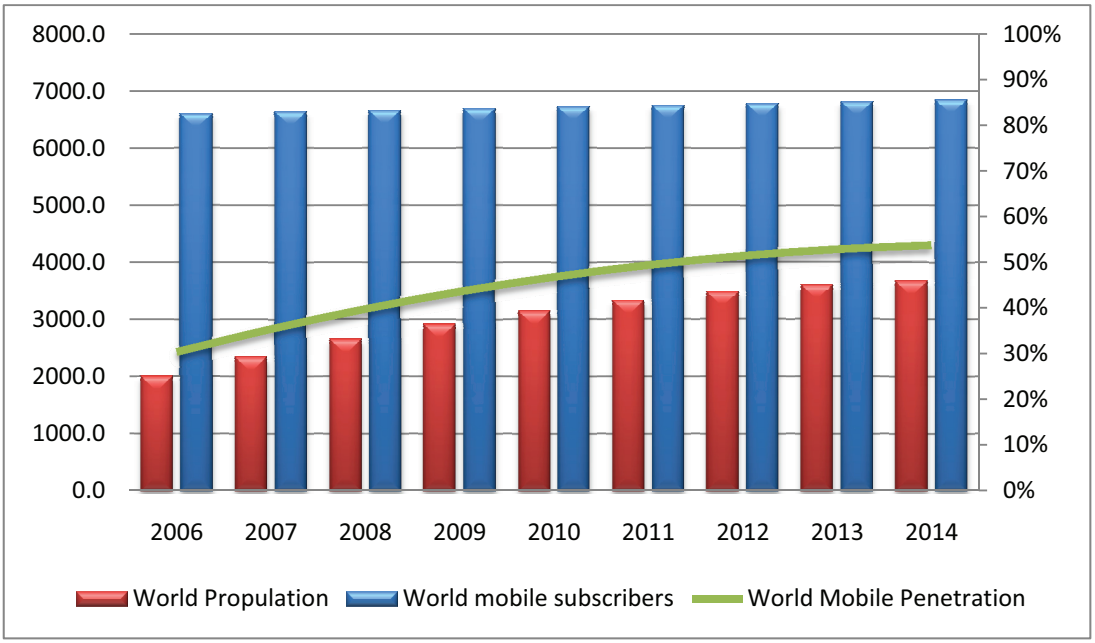
Source: Internet World Stats: Usage and Population Statistics (January 2008) www.internetworldstats.com/stats.htm (accessed 25 September 2010).

EXHIBIT 4: HDFC BANK FINANCIALS

(Figures in INR million)		
Income statement	March 31, 2007	March 31, 2006
Interest income	68,890	44,753
Other income	15,162	11,240
Total income	84,052	55,993
Operating expenses	24,208	16,911
Other expenses	31,794	19,295
Operating profit	28,050	19,787
Provisions and contingencies	16,635	11,079
Profit before tax	11,415	8,708
Balance sheet		
Capital	3,194	3,131
Reserves and surplus	61,138	49,864
Deposits	682,980	557,968
Borrowings	28,154	28,585
Other liabilities and provision	136,891	95,515
Total	912,357	735,063
Cash and balances with RBI	51,825	33,066
Balances with banks and money at call	39,714	36,123
Investments	305,648	283,940
Advances	469,448	350,612
Fixed assets	9,667	8,551
Other assets	36,055	22,771
Total	91,237	735,063

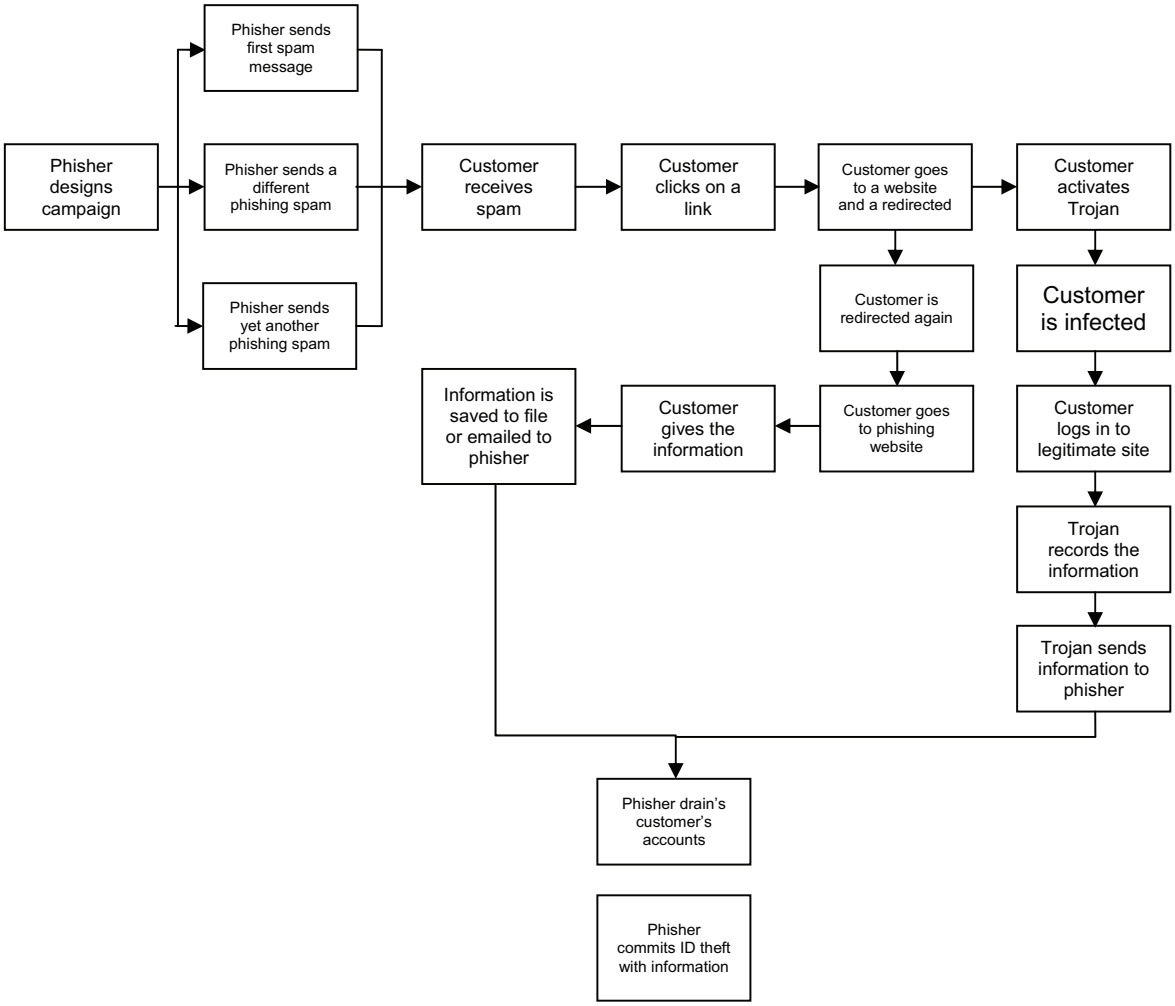
Source: HDFC Bank (2007) "Annual Report".

EXHIBIT 5: WORLDWIDE MOBILE SUBCRIBER GROWTH FORECAST



Source: "Worldwide Mobile Subscriber Growth" http://www.frost.com/industries_markets_and programs/mobile_and_wireless_communications/worldwide_mobile_subscriber_growth (accessed November 30, 2010)

EXHIBIT 6: HOW PHISHING WORKS



Source: Russell Dean Vines (2005) *Phishing: Cutting the Identity Theft Line*, Wiley Publishing, Inc, US p. 12.

EXHIBIT 7: ONLINE BANKING FRAUDS

There were nine types of online banking frauds that IT security professionals were guarding against.

Spam: This is an unsolicited, and usually unwanted, message sent to a person's e-mail account. Spam is a junk mail in an electronic form, sent in bulk.

Scam: This is an attempt to defraud a person or group of persons by gaining their confidence. The most widely known online scams are the Nigerian scam (inviting e-mail recipients to access unclaimed deposits with banks) and the Lotto scam (inviting people to claim large sweepstakes). These are again unsolicited.

Malware: This is a short form for "malicious software." Also called spyware, it is designed to invade a computer system without the informed consent of the user of the system. Malware includes any form of intrusive, dangerous and often irritating program code.

Phishing: This is a fraudulent process of acquiring sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Pharming: It is a variant of Phishing. Meant to redirect a user to a bogus website, it is usually executed by changing the host's file on the user's computer.

Man-In-The-Middle: This **i**s an electronic form of eavesdropping in which the communication with a client-server is intercepted and the user is directed to the hacker's proxy server.

Man-In-The-Browser: This is a variant of Man-In-The-Middle attack. It is in the nature of a Trojan used to infect the internet browser and has the capability to manipulate online transactions.

Replay attack: This is a form of attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Crimeware: It is a collective term for any malware developed to fraudulently obtain financial gain by capturing confidential information (like user name, password, credit card numbers etc) as part of identity theft. It is also used to capture key strokes and take control of a computer.

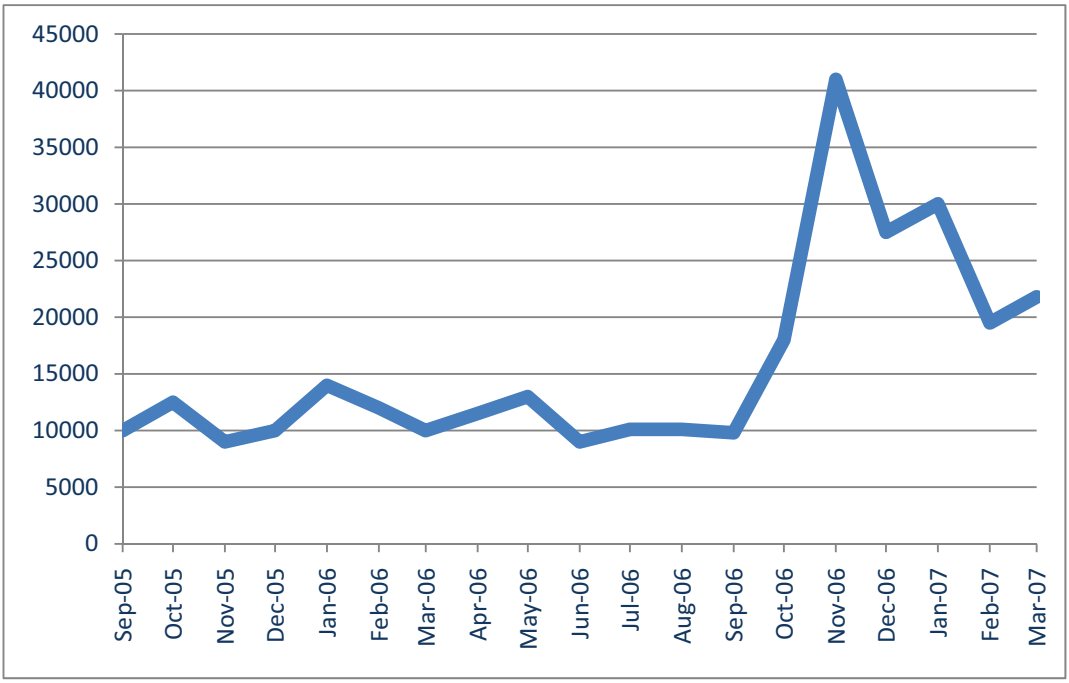
Source: http://www.en.wikipedia.org/spam; http://www.en.wikipedia. org/spam; http://www.en. wikipedia.org/malware; http://www.en.wikipedia. org/phishing; http://www.en.wikipedia.org/pharming;http://www.en. wikipedia.org/man-in-the-middle; http://www.en.wikipedia.org/man-in-the-browser; http://www.en.wikipedia.org/replay attack; http://www. en.wikipedia.org/crimeware (accessed 21 October 2010).

EXHIBIT 8: LEADING ONLINE HAZARDS IN THE US, 2006

	Frequency	Cost per incidentper person ($)	Total damages Countrywide ($)
Spam	1 in 2 people	-	-
Viruses	1 in 4 people	109	5.2 billion
Spyware	1 in 8 people	100	2.6 billion
Phishing	1 in 115 people	850	630 million

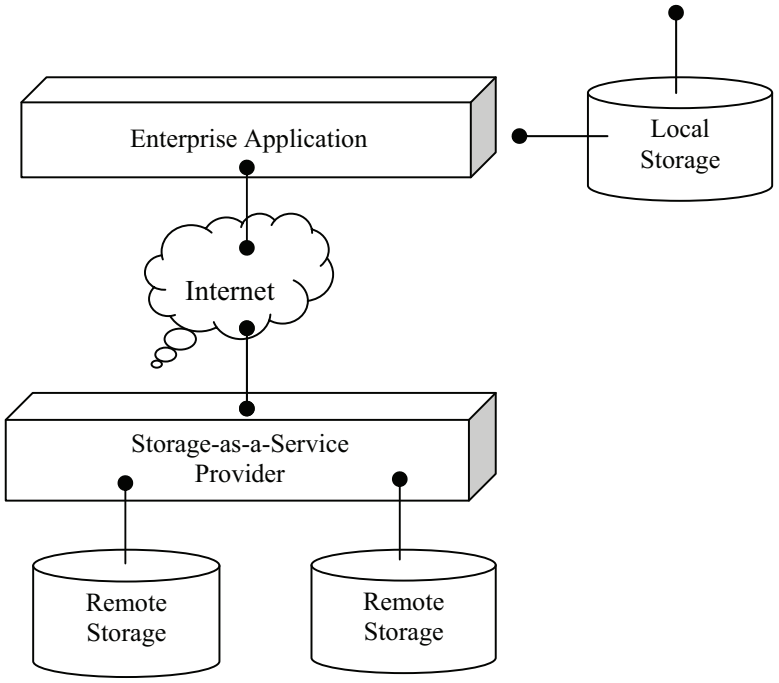
Source: Consumer Reports (September 2006) "State of the Net", http://www.consumerreports.org (accessed 5 July 2010)

EXHIBIT 9: NUMBER OF INCIDENTS OF PHISHING ATTACKS



Source: "Who is Fighting Phishing? An Overview of the Phishing Lifecycle and Entities Involved" White paper July 2007, http://www.markmonitor.com /resources/white-papers.php (accessed September 30, 2010)

EXHIBIT 10: CLOUD COMPUTING



What is cloud computing?	Consider the choice among buying a car, leasing a car and hiring a cab in order to reach a destination every day. Buying licensed software is like buying a premium car. The customer pays a fixed price, upfront. The product comes with warranty and tech support, whether used or not. Software-as-service, better known as SAS, is like paying a monthly rental. The customer gets a car of his choosing and is assured of a minimum level of service for a fixed monthly fee. But he can't add features into the car because he does not own it. Cloud computing is like flagging a metered cab. The customer pays only for the duration of the trip, without worrying about gas or maintenance. He gets there. Cloud computing is based on an architecture called multi-tenancy. A common business application, which resides in the virtual space of the Internet, is shared by everyone. It contracts and expands for every user to customize according to one's computing need. That is why it is called a cloud. Facebook and twitter are common consumer applications of cloud computing.
What are the advantages?	Cost is the major advantage. Any application that can be digitized can become a cloud based application. It can be up and running in days, or even hours. There is no capital investment or set-up cost. Managing hardware and software becomes the responsibility of the service provider. Upgrades are automatic.
What are the areas of concern?	Data security is the main concern for the customer. Reliability of infrastructure is the main concern for the vendor. The concerns are similar to what the CIOs face with physical servers in data centres.

Sources: Graphic adapted from Linthicum, D.S. (2010) *Cloud Computing and SOA Convergence in Your Enterprise: A Step by Step Guide*, Addison-Wesley, p. 39; Buckley, P. (2010) *The Rough Guide to Cloud Computing*, *Rough Guides*; Video "Cloud Computing: Plain and Simple", http://www.youtube.com /watch?v=XdBd14 rjcs0&feature=related (accessed October 5, 2010)