

Bankers As Buyers 2007

A collection of research, observations and articles about what technology, solutions and services bankers will buy in 2007 and the changing financial industry landscape

Prepared by:
William Mills Agency
www.williammills.com

The amount of news, information and research available about the U.S. financial industry and technology is staggering. *Bankers As Buyers* is compiled to help present some of that information in a logical, easy to read format. This study looks at the size of the market and the amount of money that is expected to be spent on IT and related services this year.

The focus is to help financial institutions, and those companies serving them, to validate their strategic IT direction/concerns and compare investments in technology by type and/or direct further research.

Bankers As Buyers offers findings from some of the most knowledgeable consultants and professionals currently involved in our industry. This year's survey has been greatly enhanced by information provided by or originally published by:

ABI Research
Aite Group, LLC
Celent Communications
Cornerstone Advisors
Dove Consulting
Financial Insights
Forrester Research
Gartner, Inc.

Independent Community Bankers of
America (ICBA)
Info-Tech Research Group
Javelin Strategy & Research
Reynolds, Bone & Griesbeck PLC
SourceMedia
TowerGroup, Inc.
TraceSecurity
William Mills Agency (focus groups)

While the material is copyright protected, you have my blessing to share this document with your business associates, clients, prospects and friends within the financial industry.

Sincerely,



Scott Mills, APR
President
William Mills Agency
scott@williammills.com
678-781-7201

Table of Contents

I. Spending Outlook

- A. Market Size
- B. Spending Projections

II. Spending Breakdown

- A. Fraud Prevention
- B. Regulatory/Compliance Spending
- C. Community Bank Perspective
- D. Customer Service
- E. Payment Systems
- F. Integration and the Enterprise
- G. Other Technology Spending

III. Featured Articles

Vendor Strategies in the Financial Services Sector
By Jeanne Capachin, Financial Insights, an IDC company

Top Trends Impacting Bank Technology for 2007
By Jimmy Sawyers, Reynolds, Bone & Griesbeck PLC

Emerging Bank Technologies
By Bruce Cundiff, Javelin Strategy & Research

Spotting the Fake in Identity Theft
By Jim Stickey, TraceSecurity

I. Spending Outlook

A. Market Size

According to the FDIC September 2006 data and SourceMedia*, the depository institution landscape is as follows:

	Number of
Commercial Banks	7,450
Savings Banks	1,293
Credit Unions*	<u>8,880</u>
Total	17,623

Market by Asset Size

According to the FDIC's June 30th 2006 data, the profile of banks is as follows:

Asset Size as of June 30, 2006	All Institutions		
	Number of --		Deposits (Dollar amounts in Millions)
	Institutions	Offices	
Less than \$25 Million	655	785	8,542
\$25 Million to \$50 Million	1,213	1,849	36,818
\$50 Million to \$100 Million	1,920	4,402	117,270
\$100 Million to \$300 Million	2,852	11,926	408,274
\$300 Million to \$500 Million	828	6,036	256,825
\$500 Million to \$1 Billion	654	8,021	349,490
\$1 Billion to \$3 Billion	365	8,739	443,415
\$3 Billion to \$10 Billion	156	8,382	561,357
Greater than \$10 Billion	122	44,600	4,267,437
TOTALS	8,765	94,740	6,449,427

A profile of the credit union market provided by SourceMedia is:

	Asset size (\$ Millions)	Number of Credit Unions	% of Total	Total Assets (\$ Thousands)	% of Total
Peer	<2	1,543	17.38	1,373,794	.20%
Peer	2-5	1,208	13.60	4,070,917	.59%
Peer	5-10	1,349	15.19	9,815,687	1.41%
Peer	10-20	1,292	14.55	18,515,303	2.67%
Peer	20-50	1,497	16.86	47,948,688	6.91%
Peer	50-100	774	8.72%	54,298,207	7.82%
Peer	100-250	665	7.49%	105,770,485	15.24
Peer	250-	445	5.01%	210,327,712	30.30
Peer	>1,000	107	1.20%	242,027,696	34.87
		8,880	100%	694,148,489	100%

Also according to SourceMedia:

- Credit Unions are on track to hit \$1 trillion in total assets by 2010
- At the end of 2004, there were 86 million American credit union members.

B. Spending Projections

Financial institution technology spending growth will continue in the mid single digits in 2007, continuing the trend of the last couple of years, according to technology analysts.

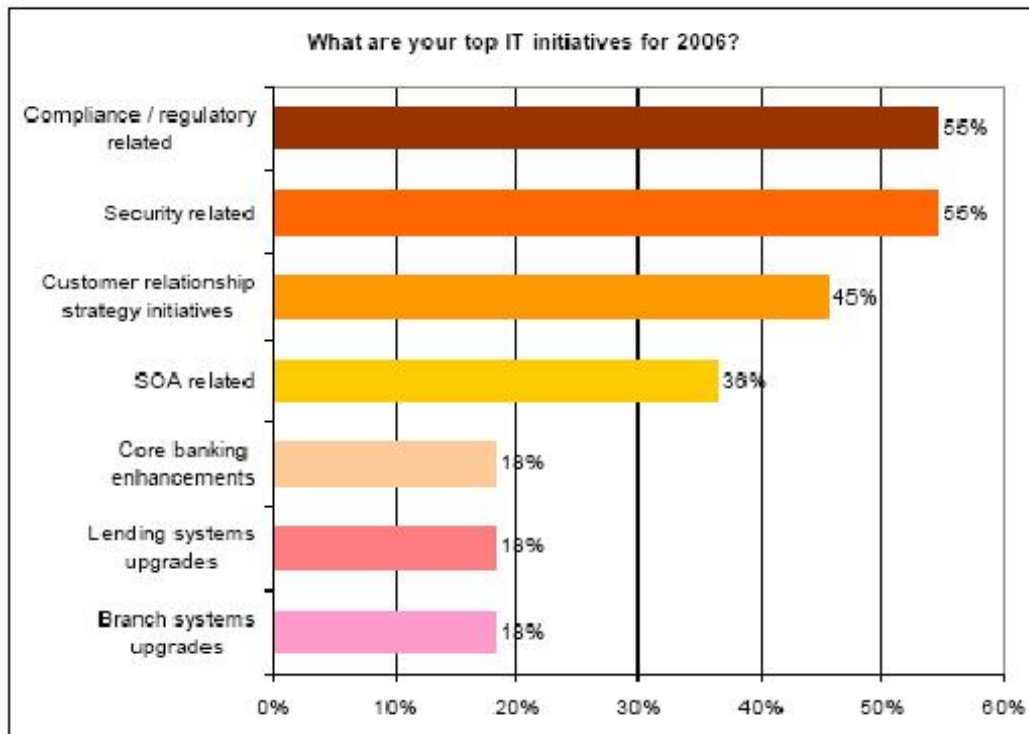
“It’s going to look a lot like it did in 2006,” said Jeanne Capachin, research vice president, global banking for Financial Insights, an IDC company. “We’re looking for a three percent growth rate.”

Other industry forecasts also expect industry technology spending to grow in the three to four percent range and agreed that many of the spending priorities that bankers had for 2006 would continue into 2007. For many banks, projects that were planned or started in 2006 will start or finish implementation this year.

Regulatory/compliance and market forces will drive most of the spending. Fraud prevention and regulatory/compliance spending are intertwined due to the need to protect customer information for legal, as well as, business

purposes. According to a 2006 survey by Celent LLC, half of all bank CIOs/CTOs say their IT budgets are “very strained” by regulatory requirements. Another one-third said that regulatory requirements were having a moderate impact on spending.

Technology spending will continue along the same priorities as 2006, with compliance/regulatory, security related and customer relationship strategy initiatives, according to Jacob Jegher, Celent senior analyst, who polled CIOs about their spending initiatives in mid-2006.



Source: Celent

“Banks have a long way to go in reducing their overall maintenance spending,” Jegher said.

Yet forward-thinking banks will be spending on much more than just compliance technology, believes Jimmy Sawyers, director of consulting for Reynolds, Bone & Griesbeck PLC, Memphis, Tenn. “I’m excited about 2007. We’re going to see a more optimistic economy overall. Innovation will be rewarded.”

According to Celent, 75 percent of bank IT spending goes to new projects, with the rest spent on supporting and maintaining existing systems.

With competition from non-bank banks such as the financial arm of General Electric and American Express, as well as direct banks, an increasing number

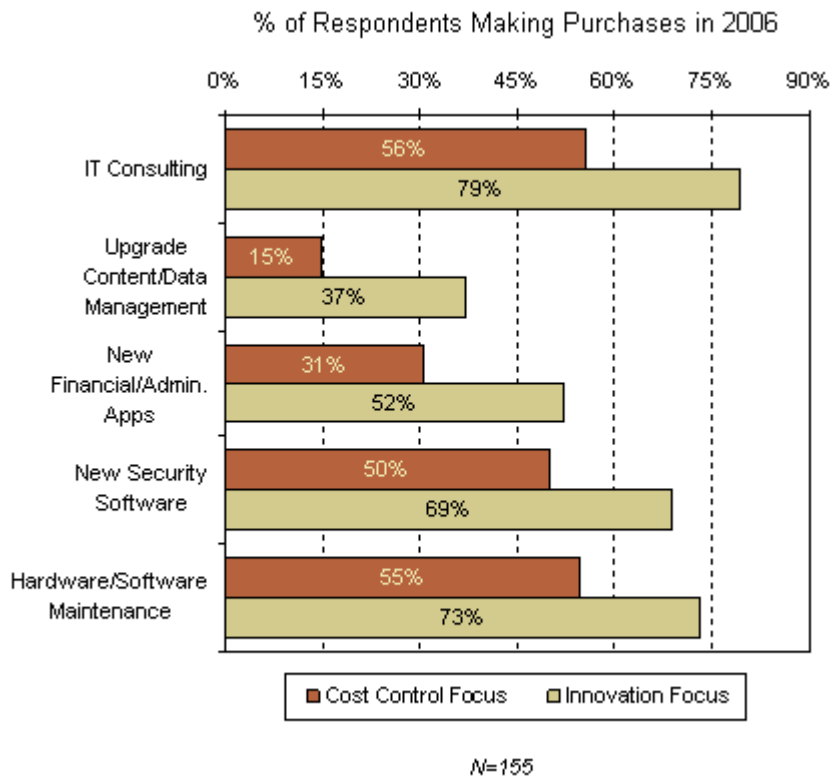
of traditional financial institutions have established direct banking arms in order to provide services at lower costs. Some of these cost savings are passed on to consumers in the form of higher rates for deposits and lower rates on credit products.

Beyond these factors, TowerGroup expects increasing consumer adoption of electronic channels and payments to drive financial institution spending in the next 12 months, a trend that will continue the spending growth pattern of the last few years.

Bank technology spending will stay level, despite shrinking in all technology spending, according to Forrester Research, Inc. After two consecutive years of eight percent growth, global purchases of IT goods and services will slow to five percent growth in 2007, reaching \$1.55 trillion in sales. U.S. purchases of IT goods and services will also grow five percent in 2007, the slowest rate of growth since 2003.

“This is a caution flag for IT vendors; 2007 will be a challenging environment,” said Andrew Bartels, vice president, Forrester Research. “Sales in the U.S., the largest single technology-buying market in the world, will be hard to come by as CIOs reduce or delay IT purchases. The single most important variable impacting future technology spending worldwide is the state of the U.S. economy.”

Banks focused on innovation will spend more than their peers on technology, according to research from Info-Tech Research Group.



“For banks to succeed in a highly competitive environment, they must learn to innovate while working within regulatory and budgetary constraints,” Jegher said.

Industry consolidation will drive some technology spending as merged institutions seek to integrate disparate systems, but won’t result in the same lift in technology spending as in previous years.

The main reason is that industry consolidation has slowed sharply, a trend that’s likely to continue in 2007.

“I suspect that has something to do with the strength of the industry,” Capachin said of the reduction of the pace of mergers. “Rising interest rates have made credit more expensive for consumers and have increased the risk in portfolios of institutions, but few if any to the point where they’re threatened with insolvency if they’re not acquired. The number of ‘problem institutions,’ according to the FDIC, stood at only 47 near the end of 2006, compared to 52 a year earlier and 80 in 2004 (the 2006 number was lowest number the FDIC posted since 1990). There is little incentive from the ‘buy’ side of the equation as well. Net interest margins and revenues remain tight, so potential acquirers aren’t flush with cash to make deals.”

“Banks are looking for more customer-centric growth,” said Jerry Silva, TowerGroup research director, delivery channels and retail banking. “For

example, Wells Fargo wants to grow from 4.5 accounts per customer to eight accounts per customer.”

“So Wells Fargo and other financial institutions attempting to grow organically will spend on technologies designed to increase cross-sell and upsell capabilities via various channels,” Silva said. “This will include technologies to provide tellers, call center agents and other customer contact personnel account relationships the customer already has as well as recommendations for additional products and services. This technology extends to interactive channels, such as at the ATM machine and via the Internet. There will be a lot of spending on analytics to gain knowledge about transactions and customers. Banks are looking at how to sell customers more products. They’re looking to make applications more interactive.”

“Many customers may start the buying process on one channel, but complete it at another, such as starting a loan application on the Internet and finishing it at the branch. But the customer doesn’t want to go through already completed steps again,” Silva said. “So banks are investing in technologies that capture and retain information in process. By learning where and why a customer interrupts an account application or similar process online, financial institutions can also identify ways to make the less costly remote channels more attractive to customers.”

Banks will also be looking to improve branch systems. Though new branches are still being built, the expansion of branches is slowing as well, according to Silva. “Bank of America had planned 500 branches over three years. It has since backed off that number.”

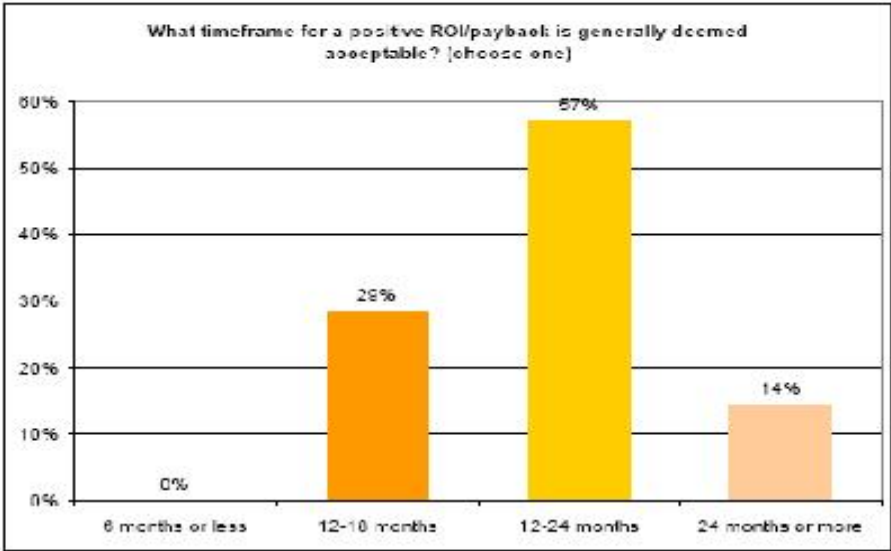
“Banks are looking at [technology] spending in smaller bites,” Capachin added. “There won’t be a lot of big investments this year. When banks do start making investments in core technologies, the spending increase will be big.”

Technology vendors, analysts and bankers themselves have discussed the eventual need to replace core systems for several years, with very few banks making changes.

Capachin doesn’t expect to see banks making such investments until new core technologies show they can save significantly on account processing costs, enabling banks to get a relatively quick return on investment.

If using current technology costs \$1 per account for processing, and a new system would reduce that to 10 cents per account, some of the larger institutions would be tempted to make the move. Some multi-national banks are already looking at new systems that will be tested in overseas markets before being considered for corporate-wide use, Capachin said. If those systems being tested by Citibank and other financial institutions overseas prove successful, there could be a strong movement to new core banking systems by the end of the decade.

According to Celent, banks look for positive Return On Investment (ROI) from technology projects within one to two years.



Source: Celent

II. Spending Breakdown

A. Fraud Prevention

“There are increasing levels of fraud and increasing consumer awareness of fraud,” said Silva. “There’s more concentration on enterprise-wide fraud management systems.”

Bankers are spending more time and money to ensure that their vendors are maintaining top security as well, Sawyers said. This becomes increasingly important as the use of “Software as a Service” increases, because banks don’t have the same control over hosted systems as they do over installed systems. This lack of control is one of the major reasons some bankers cite for continuing to buy and install applications rather than going to the hosted model.

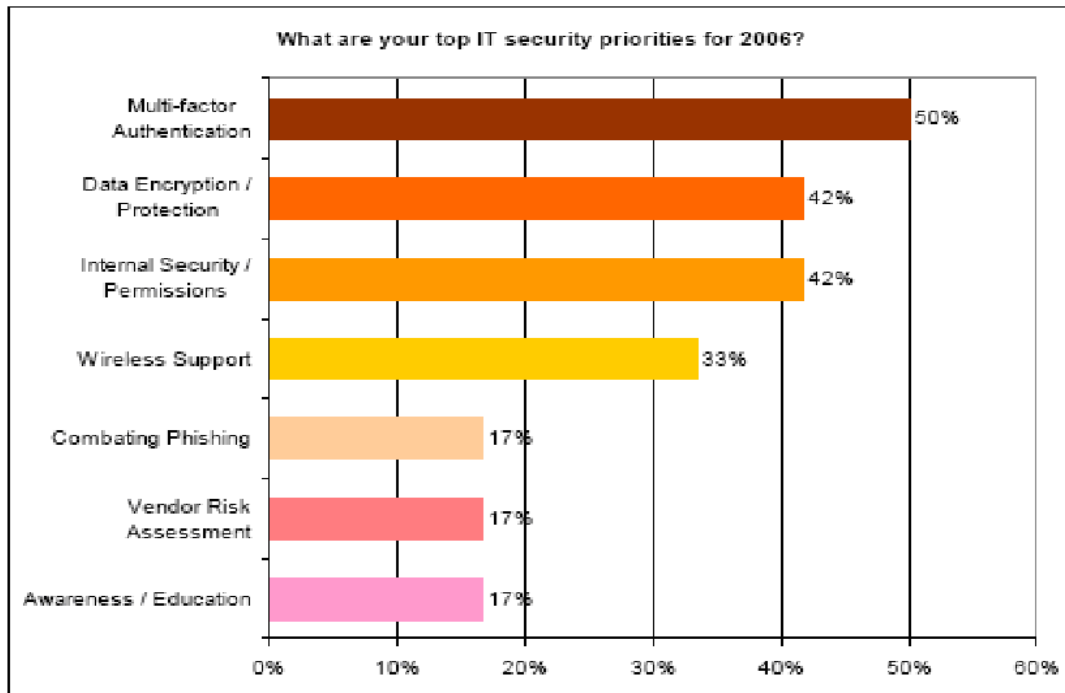
According to leading bank security vendors who participated in a Banking Security Roundtable sponsored by the William Mills Agency in the Fall of 2006, some of the top fraud/security threats are:

- Alteration of checks to increase the dollar amount and/or try to duplicate the check with some type of copy machine;
- New account opening fraud, as well as electronic-based fraud such as middleman schemes. There’s a widening range of different fraud methods that adapt to the new technologies the industry is using; and
- Embezzlement -- the bookkeeper or someone else gets a stack of a company’s check stock and writes checks from it.

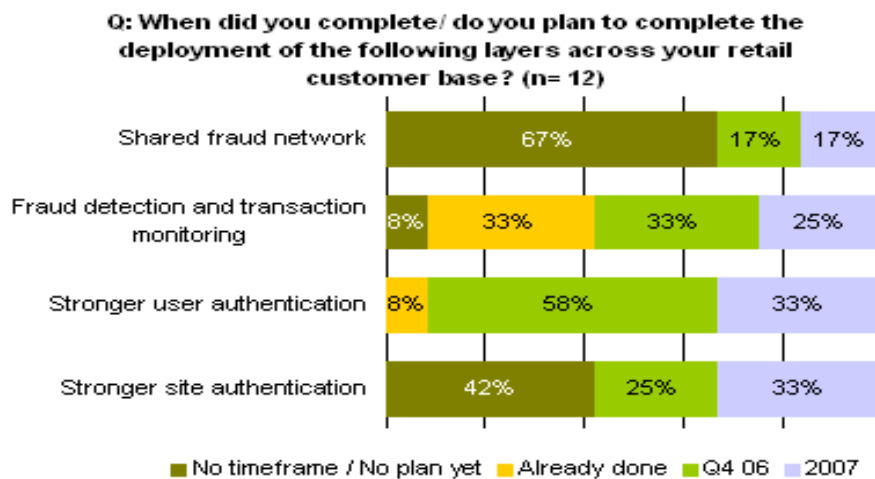
The number of phishing attacks continues to grow as well. According to the Anti-Phishing Workgroup, the number of phishing URLs grew more than 750 percent between October 2005 and October 2006. The pace of the trend is continuing to quicken.



To protect customers from the increasing amount of attacks from a variety of sources, financial institutions moved to multi-factor authentication, the technology that uses two or more factors to identify an online customer. Federal Financial Institutions Examinations Council (FFIEC) guidance recommended that all financial institutions have multi-factor authentication installed by the end of 2006. Most institutions had planned their strategies to meet this guidance by the end of last year with plans to meet it this year, according to Capachin.



Source: Celent



The perpetrators of fraud are becoming more sophisticated, working in groups, often from offshore locations that are out of the reach of U.S. authorities. So banks are investing in more advanced technologies, including exception management, intrusion detection systems and encryption.

Exception management systems enable banks to quickly recognize and confirm potential fraud from credit card charges or checks that appear to fall out of the norm for a particular customer. Intrusion detection systems monitor unauthorized access to systems and can identify breaches.

Encrypting “data at rest” helps protect financial institutions in the event of the loss or theft of a laptop, data tapes or other media that goes off premise. However, encrypting and decrypting material is too cumbersome a process for data that needs to be accessed often.

B. Regulatory/Compliance Spending

Much of the fraud prevention spending is driven by regulatory and compliance requirements regarding the protection of customer data. Despite discussions of the need for regulatory relief, particularly for smaller community banks, financial institutions continue face an increasing number of state and federal regulatory guidelines.

The influence of regulatory compliance is expected to increase and is predicted to cut into discretionary IT budgets for all types of businesses through 2008, according to Gartner. Compliance spending is currently growing twice as fast as discretionary IT budgets.

Fines issued in December of 2006 showed just how expensive it is for banks to ignore compliance mandates. Federal and Illinois regulators have fined the Foster Bank of Chicago \$2 million for violating the Bank Secrecy Act. Regulators said the bank failed to implement an adequate compliance program, including an anti-money laundering program with internal controls and independent testing. The bank did not report the transmission of millions of dollars from cash deposits to suspicious overseas beneficiaries.

The Financial Crimes Enforcement Network and the Florida Office of Financial Regulation fined the Beach Bank of Miami Beach, FL, \$800,000 for failing to implement an anti-money laundering program.

Regulators complained that the failure to follow such a program, as required by the Bank Secrecy Act, meant there were no timely reports filled of suspicious transactions that totaled more than a billion dollars.

With the myriad of federal and state rules that banks must adhere, banks rely on technology to automate as much of the compliance process as possible, but examples such as the Beach Bank incident show the importance of a

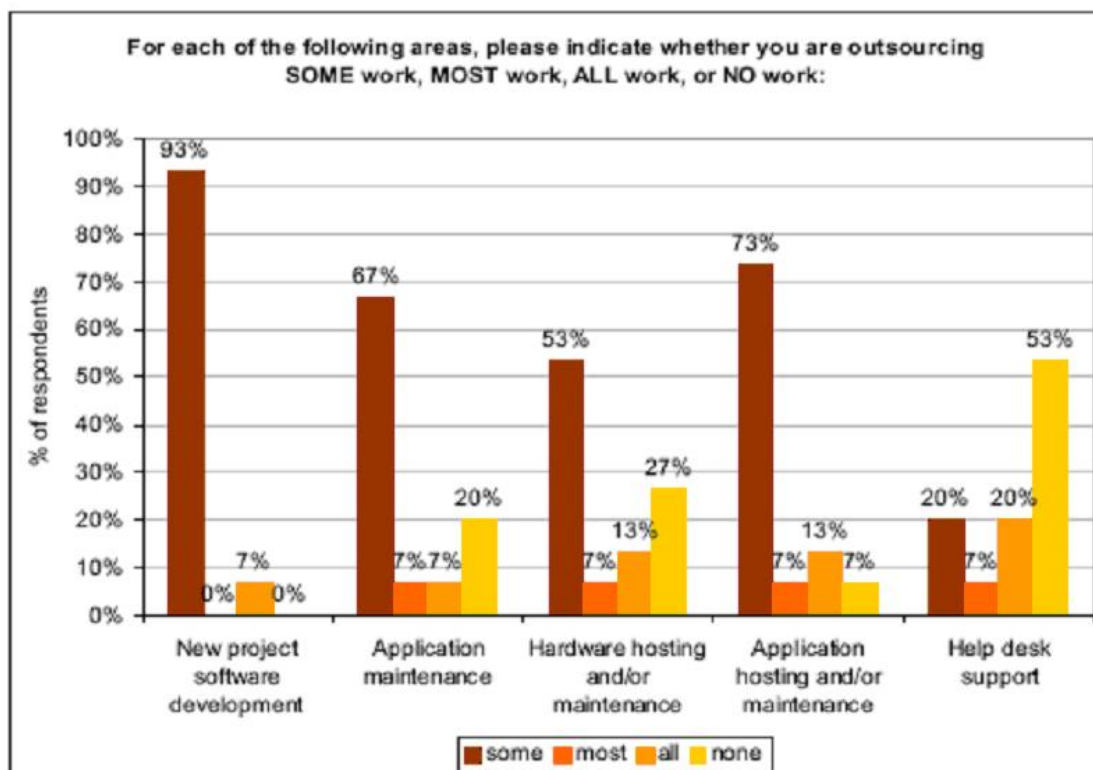
combination of humans and automation to help ensure that nothing is overlooked.

C. Community Bank Perspective

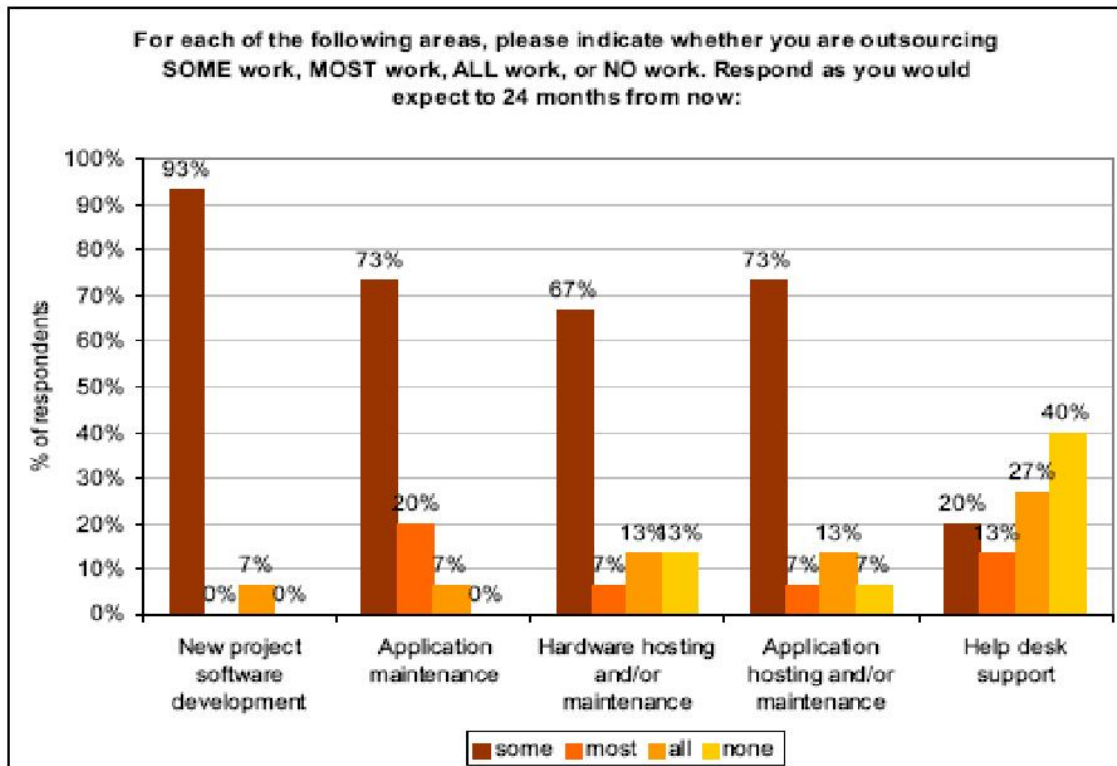
Community banks are looking at ways to grow organically, offering products, such as health savings accounts (HSA's), remote deposit capture and other products and services that only a few had offered previously, according to Sawyers. "Community banks are looking to improve the profitability of their customer base. They're running what-if scenarios to see what new programs they should put in place."

Beyond adding new programs and any supporting technologies, community banks are also moving strongly into outsourcing, or the software as a service camp, according to Sawyers.

According to Celent, 73 percent of banks use at least some hosted applications, seven percent have most applications hosted, and 13 percent have all of their major applications hosted. This trend is expected to continue, though core applications still tend to be operated in-house.



Source: Celent



Source: Celent

Some community banks have cited security concerns as the reason to keep systems in-house rather than going to the hosted model, Sawyers acknowledged. “The provider should be as trustworthy as the bank. The security [of hosted providers] should be manageable.”

Community and large banks alike tend to outsource much of their IT maintenance, according to Celent. Two-thirds of banks outsource some of their application maintenance, seven percent outsource most of this function and another seven percent outsource all of it.

A recently released survey of its membership by the Independent Community Bankers of America (ICBA) found that those with more than \$100 million in assets were facing these following long-term technology decisions:

Systems security	66%
Keeping technology affordable	62%
Data security	58%
Maintaining upgrades (existing technologies)	58%
Image-related technologies	54%

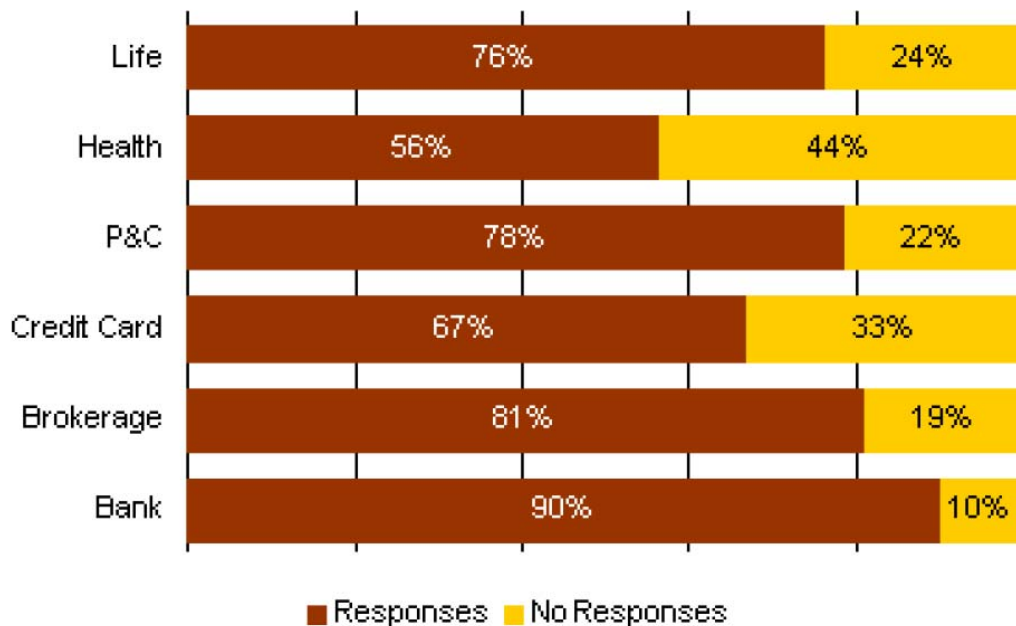
Fifty-one percent expect to spend more on technology in 2007, while another 32 percent expect the level of technology spending to remain stable. A little less than one-third (31 percent) of those banks spent between \$50,000 to \$100,000 on technology in 2006.

D. Customer Service

Banks are still working to improve customer service, according to Capachin. Efforts around this include bringing the power of more back-end systems to the front end, according to Silva. Such systems enable customer service agents and branch personnel to have all of a customer’s current data at their fingertips to enhance cross-sell and upsell opportunities when a customer calls the contact center or goes to the branch.

“Sales leakage” is losing a prospect that has started the process of buying something from you, such as, starting a loan applicant online, but not completing the sale. Sales leakage is one the most pervasive customer management problems facing retail financial institutions in the United States today, according to an Aite Group report. In a survey of 195 financial institutions (including brokerages and insurance companies), Aite found that a staggering 26 percent could not be contacted effectively online, and 77 percent of those contacted failed to respond to inquiries from prospects.

Among U.S. Financial Institutions Contacted n = 145



“Unlike other related phenomenon such as customer attrition, sales leakage remains little studied, buried into the concept of customer service,” said Gwenn Bézard, a research director with Aite Group and co-author of the report. “The way financial institutions handle incoming Web-based or e-mail inquiries offers striking evidence of the scope of the problem.”

The report reveals that nearly half (46 percent), did not address the questions. In addition, 37 percent of all respondents were unable to answer properly by e-mail, forcing prospects to use other channels such as call centers or branches.

“Human communication is not a guarantee of ‘personal touch,’” Bezard said.

A Gartner, Inc. research note points out that most customers use multiple channels, so they shouldn’t be considered “Web customers” or “branch customers.” Therefore, customer service needs to be addressed uniformly across channels. However, this also means blending different technologies, because no single one will handle the customer service needs of all channels.

Some banks are beginning to add “telepresence” systems that enable a customer to come to a branch and speak to a bank specialist who may be centrally located via an audio/visual connection that features a large, high quality screen or monitor. The idea is to enhance the customer experience so that they feel a personal connection with a specialist without the bank having to overstaff every location.

E. Payment Systems

The movement to electronic payments provides financial institutions the ability to approach payments as a profitable line of business, according to Capachin. In a report from Dove Consulting, a division of Hitachi Consulting, consumers continue to move away from checks to electronic payments, including debit, ACH and online bill payment. Online bill payments and automatic payments are rapidly gaining ground on traditional paper checks.

The result is that the Federal Reserve and other large check processors have greatly reduced their operations and shifted more of their technology spending to electronic, rather than paper forms of payment.

Banks are also using information derived from payment systems to help drive other business opportunities.

As banks become more comfortable with image exchange and other aspects of Check 21, an increasing number are attempting to leverage payments as a profitable line of business.

Check 21 permits the use of check images rather than of physical checks in the clearing process. Images are less costly to handle and transmit than paper checks and also require much less storage space. Many institutions are going beyond the strict cost-saving and efficiency enhancing features of the law to build increased relationships with and revenues from their business customers.

“The early adopters will be the ones that will reap the benefits,” Sawyers said.

Banks are in a good position to expand on this opportunity, going beyond simple check image capture, particularly for their small business customers. More than two-thirds of small businesses are interested in implementing online bill payment and invoice presentment, according to an Aite Group study.

“The more integrated a financial institution can become with a small business, the greater the understanding of their business’ needs,” says Nancy Atkinson, Aite Group senior analyst.

F. Integration and the Enterprise

Service oriented architecture [SOA] continues to be the key term, according to Silva. SOA is driving deeper into the technology infrastructure of organizations, including an increasing number of applications and systems, in some cases, even core banking systems.

“Banks are moving from point solutions to technologies that encompass the entire organization,” Silva said. Using SOA provides banks with more stable technology while enabling them to continue to get value out of older, legacy systems. “Banks are looking to bring the power of CRM systems to the front office.”

Jegher believes, 80 percent of banks are using SOA to re-engineer specific legacy applications and build them as services. Many banks who have already created services via SOA are leveraging and reusing these systems, according to Silva.

“The key word is ‘enterprise-wide,’” Silva said. “When banks consider a technology for one use, such as security, they are also looking at how to leverage the investment for other uses/departments. This helps cost-justify some technologies that wouldn’t make economic sense if installed for a single purpose or department.”

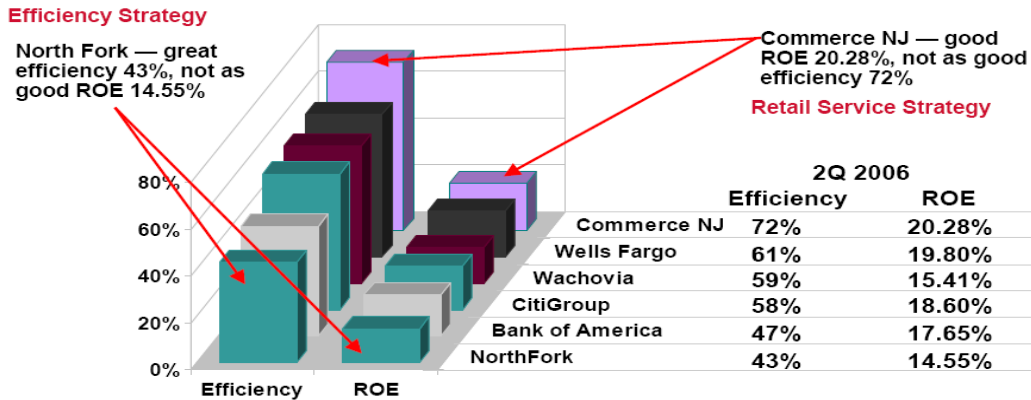
“However, using SOA, while opening up technology systems for more efficient use, also means that banks must be more attentive to rights management, to ensure that only those employees and executives with rights for certain systems have access to them.”

Financial institutions shouldn’t count too much on enhanced efficiencies from system integration or other technologies, Capachin said. “Many banks have managed efficiency with their expense hats on. Efficiency doesn’t buy ROE (Return On Equity).”

For example, Commerce Bank scores a 72 percent in terms of efficiency, topping a 2006 Financial Insights study, but had only a 20.28 percent ROE. Other banks similarly couldn’t post ROEs that matched efficiency scores.

What do Institutions Require from IT? For Starters, Efficiency Doesn't Buy ROE

Banks Must Learn to Generate New Revenues and Profits



© 2006, Financial Insights, an IDC company, All rights reserved. www.financial-insights.com

Financial Insights
An IDC Company

Integration will be an issue as some banks start considering Microsoft Vista-based systems in the second half of the year, according to Sawyers. The new operating system offers some notable efficiencies, particularly in the area of research, but may not integrate with some older legacy systems.

Others don't see Vista having much of an impact in 2007, pointing out that banks have been slow to upgrade operating systems when Windows XP, 2000, etc., have been launched.

G. Other Technology Spending

Spending on contactless payments hardware and software will reach \$870 million by 2011, up from just \$260 million in 2006, a compound annual growth rate of 27 percent, according to a U.S. study by New York-based ABI Research.

Jonathan Collins, senior analyst at ABI Research, said uptake of the technology is taking place in a fragmented manner across regions, and national markets, as contactless payments are gradually added to existing financial transaction networks.

Collins noted that in North America, open system payments are driving the contactless adoption, while in Europe contactless ticketing systems are spurring interest from payments professionals.

III. Featured Articles

Vendor Strategies in the Financial Services Sector



Jeanne Capachin

Research Vice President
Financial Insights, an IDC Company

North American banks are faced with an increasing awareness of competitive pressures. Since financial services is all about intangible assets, much of the expense that goes into delivering financial services to clients is due to investments in IT and maintaining existing infrastructure. North American financial institutions spent more than \$135 billion in external and internal IT expense in 2006, and will spend approximately \$140 billion in 2007 — this is a lucrative market for vendors that can understand how to meet the needs of this industry.

In addition to traditional IT expense, business process outsourcing a growing component of revenue opportunity on top of IT expenditure for vendors serving these financial institutions. Of the 450+ vendors Financial Insights tracks, the group of vendors with the fastest growth rates in 2006 were the outsourcing providers, led by the offshore firms. Many vendors of all stripes are profiting well thanks to the products and services they offer to financial institutions.

In 2007, institutions are now faced with margin compression, increased credit risk, lower loan demand, higher client expectations, continuing consolidation, and pressure from investors to deliver profits. However, despite these short-term issues, institutions must invest in their infrastructure to increase their ability to respond to changing market conditions and to reduce overall operating costs.

As institutions' priorities and needs change, vendors must ensure that they are aligned with the needs of their clients. There are many vendors that understand the financial technology market extremely well and have built businesses around the industry.

There is no one strategy for success in selling into the financial services industry, but there are a few proven models.

Dominance in a Horizontal Market

There are a few companies that have achieved success in financial services without developing an industry-specific strategy. These are companies that can compete by leading in their category across all industries. Although many of these companies have also developed a strategy to maximize their sales and presence within the industry, these firms have developed reputations that transcend an industry focus. Examples of companies that have this market dominance include Intel, Microsoft, Oracle, SAP, EMC and Dell. With many of these firms, a financial services strategy has followed after they have achieved success. In that case, developing a strategy to attack a market where the firm already has strong sales is about extending into more high-value, strategic opportunities. Oracle is an example of a firm that has sold its database very successfully into the U.S. financial services market and it has a well-respected brand and a strong customer base. To continue to grow in the industry, Oracle is launching a strategy to acquire more vertical-specific applications that are a good technological fit. Its acquisition of i-Flex a few years back is the most prominent example of that strategy to expand its base in the industry.

Strategic Partner

With information technology such a key component of the business of financial services, institutions always have a handful of vendors that they turn to for assistance with important strategic technology decisions. These are the vendors that are in the catbird seat — they will work with their institution clients to develop budgets, design RFPs, build business cases and advise on potential technology purchases. One way to become a trusted partner, and the most successful strategy for small institutions, is to provide the most important technology applications.

In banking, core banking providers such as Fiserv, Metavante, Jack Henry, Fidelity Information Systems, Open Solutions, and Harland Financial are perfect examples of this strategy. These firms all offer a core banking solution – the heart of banking technology. With this as the foundation, these vendors are in the catbird seat for future technology investment. Although core banking is a tough market with slow growth for now, it is the most important product in terms of building relationships, especially with banks outside of tier 1.

But being a strategic partner can take other forms as well. IBM is a strategic partner with the largest financial institutions. By developing close relationships with the executive management team, IBM has developed relationships and a reputation that provide the firm with access to the decision-making process at the largest institutions. IBM may not be the default brand that it was in the 1980s, but it is still far and away the dominant technology provider to tier 1 financial institutions.

Ride a Trend

The perception outside of the industry is that financial institutions are slow to invest and resistant to change. Within the industry, the view is much different. Financial institutions are quick to adopt technology once the business case is

proven and the technology is recognized as providing competitive success. Internet banking is a perfect example of an application that was leading edge in the 1990s and is now part of every institution's channel strategy. There were many vendors who developed Internet banking solutions for the industry, and a few are still riding on that success. Digital Insight, Corillian and Financial Fusion are examples of companies that rode that wave and grew tremendously by matching their development efforts to the demand of the market. These companies grew at a much faster pace than financial services vendors overall as they rode the adoption wave of Internet banking. The trick now for these firms is to design the second act. Internet banking is now mature and deals are fewer. For many, Digital Insight being the most recent example, acquisition by a larger firm will be that strategy. The same is true now of providers of risk management solutions that are responding to new requirements as an outgrowth of Basel II legislation. These firms are now benefiting from a high growth environment, but once institutions get through this period, growth will drop down to single digits.

Become a One-Stop Shop

Financial institutions operate in a fragmented IT environment. A large financial institution will have hundreds of software applications operating in-house or in an outsourced environment. These institutions will work with a range of IT consultants and outside developers to implement new solutions or maintain existing ones. At the same time, institutions are attempting to simplify their environments — and one outgrowth is a desire to work with fewer providers. Because institutions tend to go back to vendors with which they already have a relationship, vendors seek to increase the basket of products and services they can sell to their clients. For this reason, growth by acquisition has been very successful in financial services. SunGard, Fiserv, Metavante, Jack Henry and Fidelity Information Systems are the most prominent examples of this strategy. By building up their solution set, these vendors increase their ability to serve their customers, and in many cases, increase their stature and ability to provide strategic advice to their clients.

By following these strategies, vendors have successfully sold into the U.S. financial services market and have risen to the top. Following is a table highlighting the leading vendors in North America, ranked by the revenues they derive from sales to financial institutions of all types – banks, insurance companies and capital markets firms.

North American Financial Services Industry Qualified Revenue for the Top Vendors, 2005

Vendor	Revenue (\$M)
IBM	9,714.88
Dell Inc.	5,136.30
HP	3,787.82
Fiserv	2,952.00
Electronic Data Systems Corp.	2,368.08
SunGard	2,340.37
Cisco Systems Inc.	1,883.94
Accenture Ltd.	1,666.34
Diebold	1,376.28
Metavante Corp.	1,285.00
ADP	1,275.00
Total System Services Inc. (Synovus)	1,269.50
Microsoft	1,237.66
First Data Corp.	1,236.00
EMC	1,232.62
DST Systems	1,226.31
NCR	1,168.23
Computer Sciences Corp.	1,168.00
Fidelity Information Services	1,106.40
Sun Microsystems Inc.	1,048.65
Bisys	957.00
Unisys	874.17
Oracle Corp.	767.99
CA	719.76
Hitachi	709.69

Source: Financial Insights, 2006

Top Trends Impacting Bank Technology for 2007



Jimmy Sawyers

Director of Consulting
Reynolds, Bone & Griesbeck PLC

Get ready for an innovation explosion in 2007. All the pieces are falling into place for what promises to be a banner year for technology installations that help innovative banks leverage new technologies to better serve customers, increase employee productivity and enhance profitability.

To get your strategic plan in order and to prepare for this new wave of technology, we offer ten predictions:

Prediction # 1 - The Web Evolves Into the Platform for Business

This long anticipated “webolution” will become quite evident as 2007 will be the year the Web becomes host to a variety of applications and services. Thanks to ubiquitous Internet connectivity, wireless, and affordable bandwidth, the average user will not be able to distinguish which applications are in-house and which are Web-based.

Just as the PC of 1985 was a far cry from the PC of 1995, the Web of 2007 will be robust and ready for business. Call it Web 2.0 or 3.0, but whatever you call it there is no doubt the Web will impact your business in 2007 more than it has the previous 10 years.

Further leveraging the Web to reach the “MySpace, YouTube, Google, Starbucks, iPod, Tivo, Satellite Radio” generation, banks will discover “Vodcasting,” or video podcasting, as a way to advertise and educate. A new generation is getting their information condensed and on-demand. Vodcasting will be another method to reach this market, “connecting” not just advertising. Banking vodcasts will range from primers on Internet banking to snippets on personal finance, all designed to inform, entertain and sell. Internally, banks will embrace vodcasts to educate employees on new laws, regulations and related policies and procedures.

Prediction #2 - Technology spending increases, just in nontraditional ways

Tech spending in 2007 will increase about seven percent with the financial services industry continuing to be the biggest spender among industry sectors. However, the spending priorities will be different. Less will be spent on hardware thanks to the advent of virtualization and Web-based, on-demand applications. Expect increased spending in services, especially those related to security and infrastructure improvements. Software as a Service (SaaS) will contribute to the increase in spending.

Hardware will be further commoditized. Bankers should pay close attention to those selling “creative” hardware purchasing plans. In other words, beware the naked man who offers to buy your shirt...then lease it back to you. Unless there are compelling reasons to the contrary, leasing hardware rarely makes financial sense for banks.

Is your bank an innovator or a complier? In other words, is your bank innovating and competing or just complying and operating? Competitively speaking, innovators will stomp compliers in 2007.

Does your bank celebrate cost containment or revenue generation? Does your bank reward the person who saved money by buying the cheap axe, or does your bank reward the person who made the wiser purchase of the chainsaw, and will clearly be more productive in the woods? Many banks apply the former strategy, cutting costs at the expense of innovation. This is especially true in tech spending as bankers who fail to grasp new technologies will be left behind to scrape the bottom as low-cost, low quality providers of financial services.

Current IT budgets may not reflect many of the technologies needed to compete in 2007. Strategic technology planning will be required to upgrade bankers' visions and budgets for this new age of technology.

Writing on “risk versus reward in the long run” in their “Letter from the Founders: An ‘Owner’s Manual’ for Google’s Shareholders,” Larry Page and Sergey Brin note that “Our business environment changes rapidly and needs long term investment. We will not hesitate to place major bets on promising new opportunities.”

Successful bankers will adopt a similar long-term view.

Prediction #3 - Virtualization Changes the Networking Paradigm

To say virtualization is hot would be an understatement. Banks are enjoying the benefits of virtualization resulting in 40-75 percent one-time savings and up to 50 percent in ongoing savings. One example was an organization that consolidated 1,000 physical servers into 50. Such a 20:1 ratio may not be

typical, but 10-15:1 ratios are typical for production servers with 15-20:1 in development and testing. In the majority of installations the bank also improves business continuity efforts through server redundancy in the virtual environment.

VMware is the market leader, but others, most notably IBM and Microsoft are jumping into the virtualization market in a big way. Even the open source community is playing with XenSource claiming it can generate both Windows 2003 and Linux virtual machines with plans for Windows Longhorn in 2008.

The ability to test new applications and new releases on virtual machines before putting them into production is a significant advantage. Most banks will have virtualization in their 2007 plans.

Prediction #4 - Talented People Excel in the New World of Technology

As technology becomes more sophisticated and complex, the demand for a smart, motivated workforce will be strong. Those who update their skills will prosper. Those stuck with 80's and 90's skill sets, and who lack the motivation to learn, will suffer greatly.

Published in June 2006, ***The Cambridge Handbook of Expertise and Expert Performance*** challenges us to rethink talent as simply being gifted. On the contrary, from chess to ballet to surgery, expert performers tend to be "made" not "born." Not to say everyone has equal potential (with my vertical leap, I'm not likely to become the next slam dunk champion no matter how much I practice), but the evidence is clear that exceptional performance is typically the result of years of hard work and dedication. Furthermore, most take 10 years on average to achieve excellence in their fields. Overnight sensations are nothing of the sort. They are most likely focused individuals who spent at least 10 years honing their talents and skills.

As baby boomers retire, employers will have a hard time finding qualified employees to fill the experience gap and will turn to professional services firms to fill the gaps and provide necessary expertise. Expect partnerships such as this to grow as outside consultants complement, instead of replace, in-house expertise. Bankers will come to the realization that people don't have to work *for* the bank to work *with* the bank. Trusted providers will help banks achieve high performance through collaboration and innovation. Such co-sourcing will be a winning strategy as bankers retain loyal employees while remaining open to outside consultation and strategic alliances.

Prediction #5 - Vista Will Be the Greatest Catalyst to the PC Industry Since Windows 95

For the past 10 years, the PC industry has suffered and users have benefited from processing power that exceeds the requirements of the operating system.

Expect a reversal of fortune in 2007 as Vista emerges requiring significant hardware upgrades and planning.

There's a lot to like about Vista. Better security, a slicker interface, faster search and a 3D environment are a few key features. Vista and Office 2007 will represent learning curves not seen in recent releases. In particular, Office 2007 will require significant training. Past releases have been ho-hum events. This one is not.

Bankers should begin planning now by developing detailed software training and migration plans but wait until at least the third quarter of 2007 to deploy. This will allow banks to test application compatibility and hold out for Service Pack 1, expected in third quarter 2007.

Planning to deploy Vista on current PCs will be unwise in most cases. About half of PCs in use now will run Vista but almost all will not run Vista Premium with its heftier hardware requirements.

Regardless of Vista deployment plans, one will want to ensure 2007 PC purchases are "Vista-capable" even though one might want to run XP in the interim to ensure application compatibility. Bankers will also re-visit thin-client designs in light of Vista's requirements.

While PC lifespans have increased recently from three years to four years or more in some cases, it makes good business sense to replace PCs every three years. After three years a PC requires more technical support and experiences degraded performance. The PC may be off the books, but the total cost of ownership begins to increase dramatically and outweigh any perceived savings. Vista will drive organizations back to a three-year replacement cycle.

Looking ahead, Windows Server "Longhorn," the codename for Microsoft's next server operating system, will support 32-bit and 64-bit processing while incorporating many of the improvements associated with Vista.

Expect Vista to be adopted faster than any previous Windows operating system with 2008 seeing the most activity.

Prediction #6 - The Death of Benchmarking as We've Known It

Building IT budgets around single benchmarks simply does not work. External peer benchmarks can be meaningless when used to drive internal priorities and targets. Especially in banking, where cost accounting standards are lacking, there is no single magic benchmark that, if achieved, will bring high performance.

Aberdeen Group research found that 65 percent of poor performers leveraged a single benchmark, compared to only 5 percent of top performers who did.

Bankers will spend less time worrying about what others are doing and will spend more time investing in IT services that have the greatest business impact. Benchmarks, when used, will be viewed in multiples and in the context of relative averages not absolutes.

Prediction #7 - Bankers Remain Cautious But Confident Regarding Threats

Bankers will grow tired of unsubstantiated hysteria like the recent U.S. government warning that al-Qaida would launch a cyber-attack against online stock trading and banking Web sites. Socially awkward young men living in their mother's basement will continue to outpace al-Qaida as the real cyber terrorists. Using botnets from hijacked PCs they have infected with worms and Trojan horses, these spammers and phishers will continue to wreak havoc. More than 80 percent of spam is sent via a botnet, according to IronPort Systems. Expect more of this activity in 2007 along with more image-based spam, which now makes up more than one-third of all spam, according to Tumbleweed.

Because the greatest threats will most likely originate inside your bank, criminal background checks remain an effective tool in fighting threats to your infrastructure. Annual IT audits and network vulnerability assessments will provide independent reviews of such controls. Security solutions such as Intrusion Prevention Systems (IPS) will improve banks' security posture.

Pandemic planning will simply reinforce current business continuity plans by calling attention to any disaster that reduces workforce. Smart planning, not panic, will suffice. Preparing one's family plan will continue to be the most important issue.

Prediction #8 - Smartphones Continue to Sell But Disappoint

Poor battery life, small screens, inadequate memory, inferior as phones, slow wireless connections, difficult to secure, bulky and unstable. Other than these shortcomings, smartphones are great. These devices are the bling of the business world. They are sexy, cool and ooze gadget-envy.

Somewhere out there, in development, is the solution that will be in between a tablet PC and a smartphone. We are currently experiencing the "Apple Newton" and "Sharp Wizard" phase of the smartphone evolution. A better solution will come.

In the meantime, IT shops will have to learn to secure and support these devices as more users demand this type of communication technology. True power users will buy Blackberrys and may also buy a "real phone" such as a Razer for its voice quality, battery life, design, reliability and simple operation.

Unlike notebook PCs, smartphones tend to get more personal use making these devices an IT compliance officer's nightmare.

RIM's Blackberry continues to be the Gold Standard supplying 53 percent of the 5.2 million smartphones purchased in 2005, according to IDC.

Prediction #9 - Software as a Service (SaaS) Hits the Mainstream

Affordable bandwidth, stronger encryption and better support will make on-demand applications more popular. Salesforce.com has been the best example of SaaS but expect the model to attract bankers intent on improving their technology while reducing capital expenditures.

A small bank that might not stomach the capital outlay to implement a complete Outlook/Exchange environment, will pay-as-they-go and sign up for a per user subscription which would be easier on the budget and would further level the playing field against its larger competitors.

In the past, bankers worried about losing control of their data if it wasn't in-house. The debut of Microsoft Office Live service for small businesses may be the tipping point that makes software as a service accepted by the masses.

IDC predicts that worldwide software service spending will grow from the current \$6.8 billion market to a \$10.7 billion by 2009.

The mobile workforce will require 24/7 tech support. If the CEO's BlackBerry has problems at midnight, he or she needs help then, not eight hours later when the helpdesk opens for business. This will drive many organizations to hosted environments where such around-the-clock support can be outsourced more cost effectively

As the advent of the PC and the network led to more auditing, albeit in a more decentralized manner, SaaS will do the same. Oversight of third party providers will still be required and audits will expand in scope to cover all the bases.

Prediction #10 - Security Breaches Continue While Security Awareness and Security Solutions Improve

From the CardSystems breach in 2005 to the U.S. Department of Veteran's Affairs in 2006, it appears 2007 will continue the trend of spectacular security breaches. Most will continue to be from lost laptops, some involving third parties entrusted with confidential customer or employee information. Most reported security breaches will continue to occur at colleges and universities, not financial institutions.

Phishing and pharming incidents have scared some bankers into submission as they scrap mass email communications with customers. This is akin to

jerking the phone out of the wall because of a prank call. Cooler heads will prevail and email marketing will be recognized as an effective tool.

Clearly security awareness hasn't received the attention it deserves. Most continue to look for a panacea, but one doesn't exist. Education and awareness will continue to be key factors in mitigating security risks.

SQL and XML injections will be a growing threat as attackers breach systems using cloaked commands to read and write data from databases and other systems.

Bankers will grow weary of the seemingly endless increasing number of risk assessments required by the regulators, but over time these risk assessments will become effective tools for identifying, measuring, and mitigating risk.

IT Audits and Network Vulnerability Assessments continue to evolve in scope and increase in importance as bankers view information security as a business issue first and a compliance issue second.

Summary

2007 will be an exciting time for those involved in banking technology. From remote backup, minimalist Web sites, virtualization and Vista, to SaaS, distributed item capture, Wikis and wireless, new technology projects will shape your bank for the future.

Trusted providers will prosper. Talented, experienced people will be recognized and rewarded. Bankers embracing technology with a long term view and a sound strategic plan will enjoy sustained profitability and a competitive edge over their less entrepreneurial competitors.

To quote an Irish blessing, "May you have the hindsight to know where you've been, the foresight to know where you are going, and the insight to know when you have gone too far."

Best wishes for an eventful, yet smooth and prosperous 2007.

Reynolds, Bone & Griesbeck PLC, founded in 1916, is a Memphis-based CPA and advisory firm dedicated to providing insight, direction and solutions to its clients through informed opinion and real-world experience. Serving leading financial institutions throughout the South and across the nation, Reynolds, Bone & Griesbeck PLC is committed to the success of their clients. Call 901.682.2431 or email jsawyers@rbgcpa.com for more information.

Banks Look at Emerging Technologies



Bruce Cundiff

Senior Analyst
Javelin Strategy & Research

Emerging technologies and financial institution offerings will start influencing bank spending in 2007 and will have more impact in future years as these technologies become more evolved and more accepted by consumers.

Interactive Financial Messaging™

Customer control over account activity is about to undergo a revolution that will assist financial institutions in strengthening customer relationships and mitigating fraud. Presently, financial institutions are offering consumers the ability to opt-in to email alerts, but have yet to implement account prohibitions, or immediate “review and release” capabilities for certain transactions.

Most financial institutions are building alerts capabilities in-house, and will use vendor solutions as the complexity of offerings occurs — likely with the integration of prohibitions and review and release capabilities.

Because lack of consumer demand does not warrant financial institutions developing this functionality, Javelin foresees heightened future demand for Interactive Financial Messaging functionality in technology platforms that no vendors currently offer.

Interactive Financial Messaging is a Javelin trademarked term for specifications of financial institution communication with customers. This includes providing alerts, prohibitions for certain account activities, and review and release capabilities. The customer controls the type, frequency and parameters of the communication.

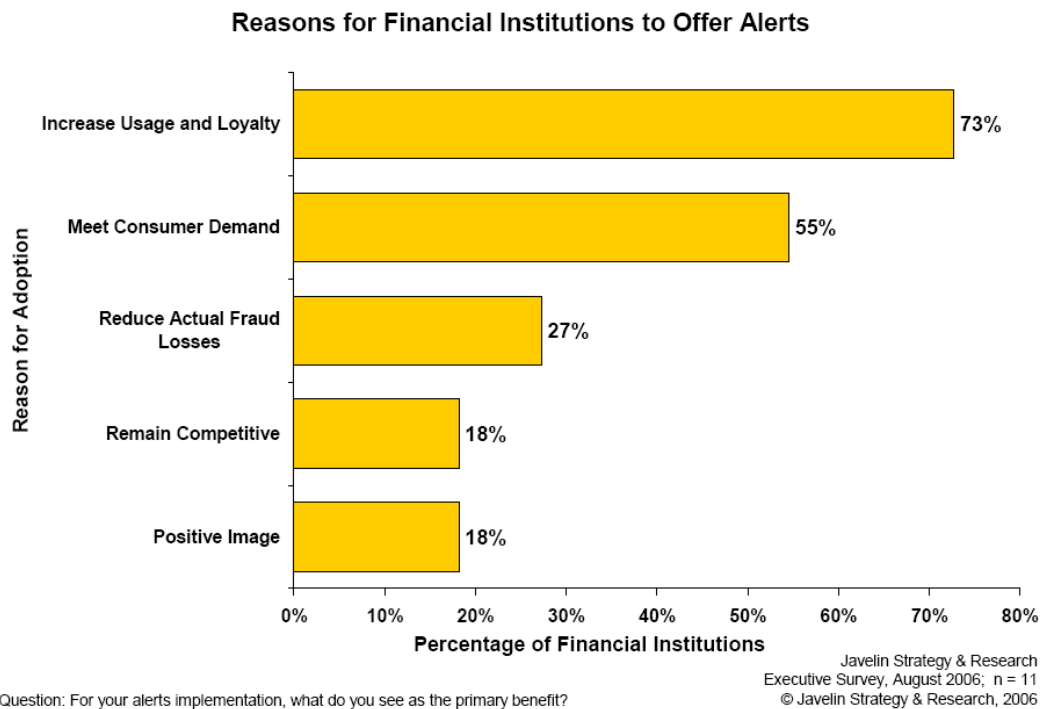
E-mail alerts are the beginning of a revolution in interactivity between financial institutions and their customers. This revolution allows for greater consumer control of account activity, will enhance relationships between financial institutions and consumers, and will strongly contribute to fraud reduction.

Presently, financial institutions are embracing e-mail alerts as a way to garner loyalty and spur usage of the online channel among account holders. All top financial institutions that Javelin surveyed have either implemented or laid plans in place to provide static e-mail alerts to customers, notifying them of particular account activity.

All programs permit consumers to choose what types of alerts they would like to receive, ranging from the account-related, such as a balance that has reached a certain limit, notification of a check clearing, or confirmation of an online bill payment, to security-related alerts, such as activity in a dormant account, or a change of address for the designated account holder.

Financial institutions overwhelmingly view alerts as a way to spur loyalty among the consumer base, with 73 percent indicating this as a primary reason for their programs.

Increasing Usage, Spurring Loyalty and Meeting Demand Drive Alerts Offerings



More than half of financial institutions are implementing alerts programs as a response to customer demand. While “remaining competitive” is cited as the primary reason by relatively few firms, the potential to lose customers if financial institutions don’t offer such programs is clear.

Complexity in account prohibitions and review and release will render the in-house build approach that most financial institutions are taking with their alerts capabilities next to impossible.

Most financial institutions indicate that an alerts engine is a relatively easy build, and they can work with much of the infrastructure that they have in place. But prohibitions require a more intricate engine — financial institutions must have a trigger in place to proactively stop action designated by the consumer on an account (wire transfers to Eastern Europe, for example).

Interactive Financial Messaging will not gain satisfactory adoption and not reach its full potential for fraud mitigation and relationship enhancement unless customers are able to make immediate preference changes “in message.”

Examples of this exist outside the financial services industry at Yahoo! and other Web sites. Focusing on the immediacy of the communication provides more control in real time for customers, and will enable the migration to, and more effective use of, next generation devices.

Health Savings Accounts

Consumer-driven healthcare is years from fruition, yet financial institutions and technology vendors must plan the right steps now to reap long-term rewards from associated products.

Less than half of consumers show an interest in HSAs (a primary vehicle for consumer driven healthcare), and most who do will seek the accounts from their employers.

Consumers want to use a card product to access HSAs for small and large transactions alike, which provides an immediate transaction fee revenue opportunity for financial institutions. Success depends on selecting HSA solution vendors that enable the simultaneous access to a multitude of financial and medical information, and also enable efficient transactions.

Organizationally, financial institutions must create HSA product management groups that incorporate expertise in payments, commercial relationships, retail relationships and asset management.

Low consumer interest in HSAs suggests that consumer-driven healthcare is still in its nascent stages. Despite an emerging focus on consumer-driven healthcare from financial institutions, legislative bodies, solution vendors and some healthcare providers, consumers will look first to their employers for healthcare plans for the foreseeable future.

Javelin data indicates that 22 percent of consumers overall, and 46 percent of those who show an interest in HSAs will seek the accounts from their employers. To date, participation in HSAs has been minimal, with roughly half of consumers indicating no interest in the products. This may change with the evolution of the products themselves, their availability, as well as the (potential) continued migration to consumer-driven healthcare.

The relationship that financial institutions have with businesses (i.e., employers) is essential for the development of HSAs. Regardless of the attempt to make healthcare more consumer-driven, the prospect of individuals seeking healthcare-related accounts, products or services — HSAs or otherwise — directly from their primary financial institutions is highly unlikely in the next three years.

Even fewer consumers would seek these products and services from a large national bank that is not their primary financial institution, from an investment company or any other entity. In the immediate term, financial institutions should leverage commercial relationships, offering HSA products primarily through businesses rather than directly to individuals.

A primary issue that financial institutions will deal with in implementing HSAs is the administrative aspect of product management. A technology layer is needed for effective implementation and management of non-financial information.

This is squarely outside the realm of financial institution's core competencies. Make certain that the technology solution analysis incorporates the ability to perform this functionality. First Data and Metavante have both created robust platforms with the idea of bringing this functionality to financial institutions.

Contactless Payments

While more rapid checkout provides some immediate market value for certain merchants, companies must search for all-important killer applications for widespread contactless technology adoption.

Embedding contactless payments in cell phones represents an opportunity for mass consumer adoption and merchant acceptance. Greater availability of over-the-air (OTA) provisioning and other technology solutions that allow for download of payment information to phones will forge this path. But networks and issuers must be certain to continuously address and allay the consumer security concerns that have arisen and will continue to develop surrounding contactless technology.

Consumers aged 18-24 show both a higher propensity to use contactless payments, greater concern with usability rather than security and an elevated likelihood of using cell phones for payment. They are a prime target for this mass adoption.

Consumer concerns surrounding contactless security may hinder issuers and payment networks in realizing the goal of contactless as the de facto technology for most card transactions.

Recent Javelin consumer data indicates that a sizeable percentage of consumers show reservations in using the technology, with 35 percent

indicating they are not interested because it seems less secure, and a further 30 percent stating that although they may use contactless-enabled devices, they are concerned that their payment information could be stolen.

For broad consumer acceptance, this perception must be overcome. Payment networks and issuers must simultaneously demonstrate the value of contactless payments to both consumers and merchants to realize widespread adoption.

Debit Card Rewards

Debit card rewards programs are emerging as a formidable tool for financial institutions to influence debit card purchase activity. This report focuses on the prevalence of debit rewards programs among all consumers, their preferences for specific reward types, and the benefits to debit issuers — including expected transaction lift — in implementing debit rewards programs.

There is currently a mismatch in debit rewards programs between what consumers want and what they are being offered, revealing untapped opportunity for issuers to realize higher returns and transaction lift.

Most consumers want cash back for debit purchases. Relatively few desire catalog points; yet catalog points are the most common type of rewards offered.

Issuers must make use of flexible platforms — provided by payment networks or built in-house — that are capable of evolving rewards programs to meet consumer demand. Debit rewards programs are not a competitive necessity.

The vast majority of consumers do not presently have debit rewards, and they are not a primary factor for switching financial institutions. Average monthly transaction lift from debit rewards is minimal in the immediate term, but grows over time. Debit issuers must build this timeframe into any individual debit rewards payback or cost benefit analysis.

Debit card issuers can expect relatively immediate transaction lift from the implementation of a debit rewards program, with those consumers who have had debit rewards less than one month indicating an average lift of roughly 1.5 transactions.

A primary reason financial institutions cite for implementing debit rewards is to grow transaction volume — to increase profitability among existing debit card holders.

Further Javelin consumer data indicates that the average monthly lift among all debit card holders — roughly 2.5 transactions — is not surpassed until cardholders have been debit card rewards program participants for two or more years. This is an important aspect for financial institutions to consider based on the payback period and revenue stream that they are expecting for debit

rewards programs. Financial institutions must factor this lift in based on the type of rewards program they plan on implementing and the associated costs.

The data and analysis presented in this article was abridged from several Javelin Subscriber reports. Javelin is the leading provider of independent, industry-specific, quantitative research and strategic direction for payments and financial services initiatives. Javelin conducts rigorous research and analysis to create successful strategies related to financial institutions, payments firms, technology vendors, merchants and billers, regulators and other policy-makers, associations, and consumer or business end-users.

For more information on Javelin or these topics, please visit www.javelinstrategy.com

Spotting the Fake in Identity Theft



Jim Stickley

CTO, Vice President of Engineering & Co-founder
TraceSecurity

Identity theft is one of the most prevalent and costly criminal activities facing individuals and businesses today. The same technology that has enabled modern-day commerce and communications has also created opportunities for illicit activities that enable identity theft. This article is to explore techniques used and suggest ways to guard against identity theft.

Recently a story was published on the [pcworld.com](http://www.pcworld.com) website that claimed “Three Florida banks have had their websites compromised by hackers in an attack that security experts are calling the first of its type.” The article (<http://www.pcworld.com/news/article/0,aid,125263,00.asp>) goes on to explain that an ISP was compromised, and customers of these banks were being redirected to malicious websites when they connected to real website addresses.

For example, a user types in the bank’s website address such as www.realbankwebsite.com. The user generally will assume that since he has typed in the correct address that when the website comes up, he is now where he expected to be. What happens is that a hacker alters the real website so when you hit the page, you are redirected to another website that looks like the real one. Only now it’s a malicious website. Suddenly you have a problem. Even the most technologically advanced user could easily fall victim to this type of attack since as far as he knew, the site was authentic.

Though the article claims these are the first attacks of their kind, in reality, very similar attacks have been taking place for years. The idea is to compromise a system at some point in a network that ultimately will redirect a user from a legitimate web server to a malicious web server. In most cases these are known as “pharming attacks.” Unlike a phishing attack, which by now just about everyone is aware of, pharming attacks are still relatively unknown and far more difficult to detect. All it takes for a pharming attack to be successful is the ability to alter a user’s DNS resolution.

DNS is used much like the phone book white pages. It assigns a name to a number. When you type a URL such as www.tracesecurity.com into a web browser, DNS will resolve that name to the IP address 69.2.40.97. This address tells your web browser where to go to connect to the website. However, what happens if the IP address being returned is altered? Suddenly you are connected to an imposter's website that is designed to look like the real website.

When most people talk about pharming scams, they refer to DNS servers that have been compromised. When your computer needs to know the IP address associated with a domain name, it will do a DNS lookup. This means your computer makes a connection to a DNS server, submits the domain you are looking to connect to, and then receives the IP address that is associated to the domain. Your computer then makes the connection to the IP address. As you can see, there is a certain level of trust that is being established between your computer and the DNS server that is sending you the IP address information. If that server has been compromised, there is no way for you to know. As far as you are concerned, you have typed in the correct URL, and you are at the correct website.

Fortunately DNS servers are far more secure today than they were just a couple of years ago. This means it is far less likely that the average user needs to worry about this type of attack.

Oh, but wait! Before you start browsing with abandon, there is another threat that is just as dangerous and much easier for hackers to perform. It turns out that just about every Windows computer out there has what is known as a host file. This file is like your own mini DNS server. As an administrator on your computer, you can modify this host file to set any domain name to be assigned to any IP address. It might sound a little nerdy, but on more than one occasion I have modified the host file on a co-worker's computer when he has walked away and forgotten to logout. My favorite is to change www.google.com to the IP address of a site that makes no sense, such as 63.99.245.32 which is the IP address for Burger King. It might seem a little silly, but you hear a lot of "What the..." type statements and other frustrated grumblings as they try to reason why suddenly they no longer can reach Google.

The problem is that it merely takes a well written active X script, virus, or other software to be run on a person's computer to modify this file. Imagine the speed at which a popular virus spreads. Now, if that virus made a change to every infected computer adding numerous DNS entries to the host file for all the major domains such as Ebay, Paypal, CitiBank, etc., the number of people compromised could be massive.

Suppose you surf through life doing your online banking, buying your favorite Pez dispenser at the online auction and all the while thinking you can trust the sites, because you typed in the names yourself. Then one day your mail arrives

and you have twenty new credit cards that are all maxed out. Now you have learned that not everything is as it seems.

Of course it's not all doom and gloom. There are a number of products on the market today that can help protect you from these types of attacks. For starters there are a number of applications, many of them free, that will monitor critical files on your computer including the host file. When this file gets modified, you get a warning message that pops up on your screen and lets you know a change has taken place. In most cases, it will even let you decline the change. Personally I like Win Patrol (<http://www.winpatrol.com>); a free application that does a number of things to help protect your computer.

There are also a number of toolbars that have been designed to protect against phishing scams. However most of these do not protect against pharming and "man in the middle" types of attacks. If you are looking to go this route, I suggest that you check out TraceAssure. Because this is put out by TraceSecurity, the organization that provides my paycheck, I will stay away from the sales pitch and just mention that this tool is free and can protect against these types of attacks.

Ultimately it should be clear that as security technology expands to protect against the threats of today, such as phishing scams, hackers are already looking toward new techniques and scams to continue their attacks tomorrow. Because these techniques can now blur the line between what you know and what you think you know, it is more critical than ever that you remain alert. If a website looks even remotely suspicious, you should contact the organization for verification. If the web site asks for confidential information, it is up to you to make the final decision of what you are willing to trust. There is no perfect solution at this point, and though security continues to get better, so do hackers.