BANK tech-trends

Financial Technology News & Strategies

Volume 1, Issue 4 November/December 2004

http://www.banktt.com

On the Inside

Is Outsourcing In or Out With FIs?

New TowerGroup (NEEDHAM, MA) research looks at recent trends in outsourcing and insourcing for the financial services industry such as the news of JPMorgan Chase's early termination of its 7-year, $5 billion IT outsourcing contract with IBM; and UBS Warburg's revelation that it would not renew the 10-year IT infrastructure management deal signed with Perot Systems in 1996.

Are the big-name mid-stream changes indications that financial institutions are "re-insourcing"? The new research from TowerGroup argues it may be too early to jump to conclusions. TowerGroup estimates that the global financial services industry terminates only 4 percent of outsourcing contracts above $250 million in advance of their expiration date.

"Two scrapped deals alone are not proof of a broader anti-outsourcing trend in the financial services industry."

"Two scrapped deals alone are not proof of a broader anti-outsourcing trend in the financial services industry," says Virginia Garcia, senior analyst in the Financial Services Strategies & IT Investments research service at TowerGroup and author of the research. "But they undoubtedly flash a signal of underlying market dynamics that may shift the balance of some current contracts, rendering them less attractive to the institution than originally envisaged."

Highlights of the research include:

- Though the two terminated outsourcing deals are essentially dissimilar, they have encouraged conversation of whether this is the start of a wider leaning to in-house IT versus outsourcing. These choices ought to persuade other organization to review the process of contract negotiations — including an insistence on variable-priced contracts, shorter checkpoints, process documentation, the right to renegotiate, and multiple contracts instead of one overarching agreement.

- Regardless of the determination of two key financial services firms to yank outsourced IT back in house, the broader outsourcing market will continue to grow at a healthy 12 percent annually. TowerGroup estimates that over the next four years outsourced IT spending will increase from nearly $28 billion in 2004 to $49.3 billion in 2008.
- TowerGroup believes the "megadeal" will change in three fundamental ways —
  - ♦ The primary driver to pursue large outsourcing deals will shift from cost savings to enterprise transformation;
  - ♦ FIs will pursue more deals targeted to specific vertical and horizontal IT functions ;
  - ♦ Traditional outsourcers such as IBM, CSC, and EDS will have to make increasing room for non-traditional offshore vendors such as Infosys, Wipro and Tata Consultancy Services.
- Large outsourcing deals will not go away because they have a high price tag. Rather, they are going to go away if they are too broad, and therefore unmanageable.

"We believe up to 80% of outsourcing contracts are not meeting desired expectations, due to inability to meet cost savings goals or less obvious issues like underutilization of contract capacity," says Garcia.

Using Flexible Account Analysis Solutions

More and more banks are boosting revenues and reducing expenses by fully-utilizing the robust flexibility of today's account analysis systems. Many of the older, mainframe-based systems are limited in their ability to set up customized pricing plans for individual accounts or groups of accounts. The latest systems, on the other hand, provide greater flexibility by allowing a system user to define varying price, rate, and processing options for different banks, geographic areas, industry segments, account types, or individual customers. They also offer the ability to significantly reduce mailing and printing costs by providing customers with account analysis statements over the web. Banks that have implemented these new systems have typically been able to increase revenues by 5% or more by charging for services that they previously were unable to capture and also providing incentives to customers to maintain larger cash balances.

The account analysis systems used by many banks are limited in their flexibility. For example, if a bank holding company is processing multiple banks in a rigid account analysis system, it may only be possible to set a single standard price for each service code by bank. That price then applies across the board to all of the customer relationships. To get around this problem, a holding company may set the price for each service at the highest level offered by any of its banks, and then individually discount the price for customers of each of the other banks. But often there are limitations on the number of individual pricing exceptions that can be made. In the very frequent case where the loan officer wants to provide special pricing on additional items, it may be necessary to discount the entire relationship, resulting in a larger decrease in revenue than required. Making more complicated changes, such as instituting a tiered earnings credit rate, could require a long and expensive customization process.

More Information Than in the Past

Today's cutting edge systems also provide substantially more information than was easily accessible in the past, such as profitability at both the service and customer levels, variance reporting, trending, audit trails, and, in some cases, an ad-hoc query tool allowing a bank to customize report data in a truly meaningful way. They also make it easy to provide customers with their account analysis statements in Electronic Data Interchange (EDI) 822 format. Additionally, newer systems can also save time by automating the process of posting billing feeds into the account analysis system. Upstream data from the bank's ancillary systems, captured either manually or systematically, can be reformatted by the account analysis application to facilitate this automation.

After all of the analysis data has been captured and posted to the account analysis system, the initial analysis run can typically be completed in just a couple of days. The relationship managers and customer support groups then have a window to review the statements and make adjustments. The review process allows them to quickly identify and report any error, long before the statement is delivered to the customer.

With the new account analysis software, banks can create and test new pricing scenarios simply by changing parameters in the software. Each year, banks traditionally re-visit their pricing schedules to modify the pricing and product mix. A robust account analysis system will allow the bank to perform what-if modeling on the bank's analysis portfolio to see firsthand the effect such modifications will have on the bank's bottom line.

Better Pricing

"The new generation of software has substantially increased our ability to price our products according to market conditions," said Priscilla Dougherty, Vice President and Manager of Client Services and Account Analysis for BOK Financial Corporation (a multi-bank holding company based in Tulsa, OK with $13.1 billion in assets). "We now set prices differently when appropriate for each of our different banks and sometimes for geographic regions within each bank's territory. When necessary, however, we can easily change pricing for individual customers and there is no limit to the number of special prices we can offer. The new software also gives us the ability to set expiration dates for pricing which helps to alert us that a customer's contract has expired and needs to be renewed. We have seen a number of cases where we have won new customers that we would have lost in the past due to inflexible pricing. Our projections when we purchased the software were that we would be able to quickly recoup its cost through increased revenues. These estimates were very conservative and it looks like we should have no difficulty in exceeding them."

Improved Efficiency

Mike Blake, Assistant Vice President and Business Analyst for BOK Financial added that the move from outsourcing to purchased software has significantly improved efficiency. "In the past, we were at the mercy of our outsourcer's schedule as to when they could get the account analysis done," he said. "Now we can run the job in far less time and make corrections at our convenience. The new software reads a standard formatted file produced by our banking software and posts them into its database. The process is nearly entirely automated. Our account service then reviews the statements and makes any necessary corrections. With the new software, account management can make changes in pricing scenarios without any programming simply by changing parameters in the software. The software makes it easy to provide management with any information they want to see, including detailed breakdowns of the impacts of discounts on our pricing by customer or by service.

New Pricing Scenarios

With the new account analysis software, the Product Management group at Sovereign Bank (the third largest bank serving New England with $40 billion in assets) was able to create and test new pricing scenarios simply by changing parameters in the software. "We created a tiered pricing system so that customers begin receiving an earnings credit when their investable balance exceeds a preset threshold, and increases as the balance increases," said Cindy Fisher, Product Manager and Assistant Vice President, Sovereign Bank. "This encourages them to hold higher balances in their accounts, and compensates them appropriately when they do. We haven't seen a dramatic effect yet from this move because interest rates are so low. But as rates rise, we are expecting to see a very favorable impact on our bottom line. Conversely, we were able to create an overdraft interest charge to compensate us when we fund customer use of uncollected deposits."

> *"The new generation of software has substantially increased our ability to price our products according to market conditions."*

Sovereign is also in the process of taking advantage of the new software's ability to provide account analysis statements over the Internet. At present, the relationship managers and customer support groups review these statements over the bank's intranet so they can spot and correct any anomalies before they are delivered to customers. Sovereign made the web version of the account analysis statement look nearly the same as the print version. The final statements are sent to the intranet site so they can be viewed if a customer calls with questions after receiving their mailed Analysis Statement. This has become a very valuable research and customer service tool.

The bank plans to roll out web access to customers in the near future. This represents a tremendous cost savings opportunity because of the huge amount of money spent by Sovereign and most banks to print and mail statements to customers. A recent survey indicated that 22.4% of all labor hours for a typical bank were involved in rendering statements and checks. Estimated total annual costs to deliver statements to a single customer are in the range of $7 to $15. "Sovereign spends a significant amount in mailing and printing costs yearly," Fisher said. "We conservatively estimate that through a combination of pricing incentives and convenience about 10% of our customers each year will choose to receive their statements over the web."

Helps with Corporate Accounts

The new software also makes it easy to fulfill the requests of large corporate customers to electronically transmit account analysis statements using the standard Electronic Data Interchange (EDI) 822 format recommended by the Association for Financial Professionals (AFP), formerly the Treasury Management Association (TMA). The account analysis statement for any customer can be quickly reformatted into the standardized electronic file available for secure download from the bank's web site.

"With our new pricing structure in place for only a relatively short period of time, and our web account analysis statements about to come on line," Fisher said, "it's still too early to quantify the costs and benefits of moving to the new account analysis system. But we have already seen cost reductions through automating the account analysis process, and are expecting even greater savings once the web statements go online and we begin reducing the number of statements that we are required to print and mail. For these reasons, it's already possible to label the initiative as a clear success that will continue to pay dividends for years to come."

Thanks to Don Enright, Sr. Sales Executive at The Weiland Financial Group, Inc., (www.weiland-wfg.com for contributing this article. Contact Don can at (847)735-0577, or sales@weiland-wfg.com.

Guidance Proposed on Overdraft Protection

On June 7, 2004, regulatory agencies released a joint proposal to address the increase in consumer use of overdraft protection: Interagency Guidance on Overdraft Protection Programs, Federal Register Vol. 69, No.109, pp 31858-31864 (June 7, 2004) and Proposed Amendments to 12 CFR Part 230 (May 27, 2004). The agencies are proposing to increase consumer disclosure and to force banks to better measure and manage the attendant credit risk. If implemented, financial institutions will require certain minimal functionality to facilitate compliance.

The primary disclosure proposals which will require systems solutions are:

- A requirement that consumers be notified of an overdraft caused by a non-check transaction (including an ATM withdrawal or debit card purchase) and allowed to cancel the transaction prior to overdrawing the account; and
- A requirement that account statements include monthly and year-to-date totals of all overdraft and returned item fees. Itemization of these charges would be voluntary.

The proposals related to credit risk management will require an institution's systems to generate specific reports and flag certain transactions, including:

- Management reports detailing overdraft product volume, profitability and credit performance;
- Reports identifying consumers who present a credit risk by relying too heavily on overdraft protection; and
- Identification of overdraft balances over 30 days so that an institution can reclassify them as loans and write them down.

These proposals will surely meet stiff resistance from the banking industry. If finalized, they will present yet another opportunity for the financial technology industry to provide automated solutions to regulatory challenges.

Thanks to Rusty Pickering and Scot Kees of Nelson Mullins Riley & Scarborough, LLP (Atlanta, GA) for contributing this article. You can contact Rusty at 404-817-6117 or rusty.pickering@nelsonmullins.com; or visit their website (www.nelsonmullins.com).

Hypercom, SiVault Launch HBNet

Hypercom Corp.'s (Phoenix, AZ) HBNet, Inc. subsidiary announced an agreement with SiVault Systems (San Jose, CA), which provides secure storage and retrieval of signed documents and biometric signature-based authentication. The companies will implement Hypercom's HBNet information delivery *service to provide high performance transaction processing speed, convenience, and security to the medical, financial, and retail communities.*

SiVault Systems' also intends to combine its end-to-end signature verification technology with Hypercom's high-speed Optimum L4100 signature-capture card payment terminal. Hypercom terminals process transactions via dial or Internet Protocol (IP) at the point-of-interaction in retail

"HBNet gives us unique capabilities to support high-speed processing and multiple front-end technologies with a no-single point of failure architecture at very competitive prices," says Emilian Elefteratos, SiVault Systems chief executive officer and president.

"Consumers are demanding speed, superior service, and security - especially in today's fast-paced environment - and retailers nationwide want to meet that demand. Now they can do it with HBNet's high performance transaction delivery network, Hypercom's card payment terminals, and SiVault Systems' end-to-end signature verification technology," states Sharon Cline, senior vice president and general manager, HBNet, Inc.

Hypercom's HBNet network for North America's dial and IP POS market handles authorization and electronic transaction-processing retail point-of-sale for financial, government, healthcare, and other transaction-based markets. Ultra high-density MegaNAC® 180 Network Access Controllers (NACs) strategically positioned within the North American Public Switching Telephone Network (PSTN) and at processor data centers, power the HBNet transaction network.

Cyota Identifies New Bank Phishing Hole

Cyota (New York, NY), an anti-fraud and security solutions provider for financial institutions, revealed a significant adjustment in the swiftly mounting phishing problem. Fraudsters are now aggressively attacking banks that were previously under the phishing radar and hitting them in mass numbers.

At first phishing attacks focused on a few of the largest financial institutions, but recently As the leading banks have begun to deal with phishing and deploy solutions there has been a change in the financial institutions under fire. In addition, in the past phishers would slowly amplify the number of attacks on a certain bank. Now, Cyota's Anti-Fraud Command Center (AFCC), which monitors online fraud on behalf of Cyota's clients, has identified that phishing attacks have not only targeted different banks but they are doing so at an alarming rate.

Cyota's AFCC recently spotted several such cases where within three months fraudsters launched hundreds of attacks, compared to 1-10 attacks total against the same entities previously. For example, over the past three months, several large to mid-sized banks in the U.S have seen a growth of thousands of percents for attacks against them. For example: one mid-sized American bank had 283 attacks in October compared to 10 attacks in August.- a growth of 2,800 percent , and a top-10 American bank had 107 phishing attacks in October against just one in August, a jump of 10,700 percent .

The distinctiveness of this trend and what causes alarm is that fraudsters attack the less-suspecting targets with 'surprise attacks' - multiple, subsequent hits, thus catching some financial institutions off guard and capturing as much stolen information as possible in a very short timeframe.

"Banks can no longer assume that they will have time to better protect themselves after their first phishing incident. They must be pro-active in preparing in advance as phishing and online fraud continue to evolve and spread with little early warning," says Amir Orad, Cyota executive vice president of marketing.

S1 Suite Deal with Mosaic Adds ATM Channel

Atlanta-based S1 Corporation, a provider of integrated front-office applications for financial institutions, announced that it has reached a definitive agreement to acquire U.K.-based Mosaic Software Holdings Limited, which provides technology that drives ATMs and electronic payments. The acquisition enables S1 to offer financial services providers an ATM channel solution along with the S1 Enterprise integrated front-office suite, which includes the branch, call center, Internet and voice customer interaction channels.

Mosaic-developed solutions provide processing for electronic financial transactions. These solutions directly control ATMs, intercept cardholders' bankcard transactions, and process these transactions online to core system accounts. Mosaic software enables banks, as well as by non-traditional financial service providers, to provide multi-function ATMs to customers for initiating transactions for money orders, transfers, pay check deposits, and bill pay. Mosaic's software also manages payment authorization transactions initiated through point-of-sale (POS) devices, online retail sites, and Web-based call centers.

S1's ATM solution will be available independently or as a component of a complete solution that gives banks one view of customers across channels.

PIN Pads Getting 3DES-ed

Even with video cameras, audit trails, and steel reinforced cash vaults, wily thieves armed with social engineering techniques and street technology still managed to take home some $50 million last year in ATM crimes in the US alone, according to estimates by the Electronic Funds Transfer Association (EFTA). The credit card associations are doing their part to fight back, especially in regards to PIN entry devices (PEDs).

The humble PIN pad is undergoing major changes. For example, last year Visa International formally launched a 50-point security certification process for PEDs on ATMs that accept Visa. The review is exhaustive: an independent laboratory opens up the PED and probes the electronics; it examines the manufacturing process that produced the device; it attacks the PED as an adversary might, monitoring it, for example, to ensure that no one can identify which buttons are being pressed by sound or electromagnetic emission. This thorough process can last up to four weeks and is handled by only three certification labs approved by Visa worldwide.

The modern PED is a physically and logically self-contained, tamper-resistant unit that encrypts a PIN within milliseconds of its entry. The plaintext PIN never leaves the unit, never travels over the network, isn't even available to the ATM's processor; malicious code running on a fully compromised Windows-based ATM machine might be able to access the cash dispenser and spit out twenties, but in theory it couldn't obtain a cardholder's unencrypted ATM code.

The credit card companies have played a large role in advancing the state of PED security. Visa's biggest rival, MasterCard, naturally has its own certification program. They have mandated an April 1st, 2005 deadline for ATMs that accept its card to switch their PIN encryption from DES to the more secure Triple DES algorithm (some large networks negotiated a more lenient deadline of December 2005.)

But despite these efforts, ATM fraud artists are becoming increasingly sophisticated. For example, they use specially-constructed sleeves inserted in an ATM's card reader that physically captures the user's card. The con artist then lingers near the machine and watches as the frustrated cardholder tries to get their card back by entering their PIN. When the customer walks away, the crook removes the sleeve with the card in it and makes a withdrawal.

At an even higher level of criminal sophistication, police have found ATMs affixed with a hidden magstripe reader attached to mouth of the machine's real reader, expertly designed to look like part of the machine. The rogue reader skims each user's card as it slides in. To get the PIN for the card, swindlers have used a wireless pinhole camera hidden in the ATM fascia or a pamphlet holder and trained on the PED, or attached fake PIN pads affixed over the real thing that store the keystrokes without interfering with the ATM's normal operation. Afterwards, they can easily create a phony card and use that PIN.

Visa's certification requirements try to address this hardware-assisted fraud. Under the company's standards, each PED must provide "a means to deter the visual observation of PIN values as they are being entered by the cardholder." And the devices must be sufficiently resistant to physical penetration so that opening one up and bugging it would either cause obvious external damage, or require that the crook take the PIN pad home with him for at least 10 hours to carry out the modification.

Visa originally set a July 1 deadline, but was forced to back down because it was not realistic for manufacturers to redesign and test their pads. So the association has suspended the deadline and fortunately is now working with MasterCard to develop an industry-wide standard before setting a new deadline for mandatory compliance. Meanwhile, Visa is encouraging vendors to submit their PIN pads for certification under the old requirements voluntarily, for the sake of security. With all of this work being done on the PEDs, banks can feel pretty secure in knowing that their ATMs will be more secure.

Intrusion Prevention Options Growing

Intrusion prevention software (IPS) has been available to organizations for some time, but big changes are in the offing with new products hitting the market. Products like ZoneLabs Integrity, ISS RealSecure, Sana Security's Primary Response IPS, Cisco's Security Agent and McAfee's Entercept have been around for awhile, but eEye Digital Security is claiming to one up everyone with their new defensive suite called Blink. eEye says that Blink uses a different and more effective approach than other intrusion prevention software.

Here is a quick overview of the various places where intrusion prevention software can reside:

- The Process Layer. This is the conceptual area where software applications run, whether on a corporate server or on a PC. "Host-based" intrusion-prevention software (HIPS) can monitor the processes within machines and attempt to detect and halt unusual behavior that suggests a possible hacker attack.
- The Network Layer. The "network layer" is the portion of an operating system that is closest to a machine's hardware connection to the Internet or a local area network. Blink carefully monitors activity in this layer to stop attacks, eEye says, before they ever get a chance to interact with processes and applications.
- The Hardware Layer. Every machine that is connected to a network has some kind of networking card that handles the physical tasks of communication. "Network-based" intrusion prevention systems (NIPS), which defend at the hardware layer, usually take the form of a physical appliance that's installed between the Internet and the networking card on corporate servers. Although they can be effective against external attacks, network-based defenses can't protect against rogue applications that may be running within an organization's PCs or insiders who seek unauthorized access.

The recently released Blink software protects the network layer of the operating system against unusual activity - without relying on a list of attack "signatures." This preventive capability, plus eEye's new application- and system-level software firewalls, plus its Retina vulnerability assessment tool (which has been available in some form since 2000), have been combined to form Blink.

The bad news is that Blink needs to be installed onto every server and client PC in an organization. A deployment this broad is a daunting task for large banks, but once Blink is widely installed it offers enterprise-wide manageability with centralized dashboards and policy setting, eEye says. They tout the following benefits:

- Defense Against "Zero-Day" Attacks. Blink's behavior-monitoring approach means that PCs running it are protected against new assaults, known as zero-day attacks, that take advantage of previously-unknown vulnerabilities for which no vendor patch is available. Using this technique, eEye's software was able to hold off such widespread exploits as Code Red and LSASS.
- No More "Panic Patching." When patches for newfound security holes do become available from software publishers, it may not be necessary for enterprises running Blink to install those patches on a crash basis to prevent a successful intrusion. If Blink is already guarding against a particular hacker exploit, installation of the new patches can wait for the next regular maintenance cycle, saving labor and downtime costs.
- Protecting Roaming Laptops. A mere "security perimeter" approach to defense is flawed because workers routinely take their laptops and other portable devices outside the perimeter. When these devices return onsite and are again plugged into the local network, any Trojan-horse software they may have caught has an opportunity to probe across the LAN for vulnerabilities. Installing Blink on mobile devices helps defend them from attack when they are off the network.

eEye officials believe their new software approach offers better overall protection than other intrusion prevention software. Naturally, their competitors beg to differ. For instance, security vendor PivX Solutions thinks that their new IPS offering, Quik-Fix Pro, has advantages over the layered approach Blink uses. Quik-Fix Pro, the company says, acts like a series of patches for Microsoft Windows and numerous Windows applications that otherwise would be susceptible to stealthy intrusions. It is difficult to sort out the various claims of all of the IPS vendors, but one thing is certain: any intrusion prevention system is

Boosting WAN Performance

The Transmission Control Protocol requires an acknowledgment of each packet, and if that acknowledgment is slow or fails to come, the sending machine throttles back its transmission rate, assuming the link is congested, even if it's not. One company claims that this can result in WAN (wide area network) connections running at only 20% of capacity because of packet loss across the link.

Start-up Orbital Data is launching gear that it says boosts throughput on WAN connections 10 times or more by overcoming bottlenecks caused by the limitations of TCP. Called Orbital 5500, the appliance is sold in pairs with one at each end of a wide-area link, where they optimize TCP sessions so transmissions fill the available pipe rather than sending at the slower speeds that TCP normally dictates.

To eliminate this, the company uses a feedback mechanism between its devices so traffic is sent at the speed of the connection. This is done using Orbital's own flow-, congestion- and retransmission-control algorithms and buffers in the boxes. When traffic is sent across a WAN, it is sent using standard TCP. Orbital Data calls its technology Total Transport.

Other companies are also in the WAN optimization business. Competitor Peribit Networks' WAN gear adjusts TCP receive-window size to maximize throughput across WAN connections. Peribit gear also compresses traffic. Another start-up called Aspera sells software that sends WAN traffic using a proprietary transport mechanism other than TCP. Riverbed Technology spoofs protocols to reduce the number of transactions necessary to complete a WAN transfer, thereby reducing the total number of packets crossing the connection.

Orbital 5500 is managed via a Web interface on each device. The devices are placed between the LAN and the WAN, and if they fail, traffic passes through as if they weren't there. Pricing ranges from $12,000 for T-1 throughput to $50,000 for 200M bit/sec throughput. Orbital has good funding and their CEO, Richard Pierce, is the former COO of Inktomi.

Faster, Smaller Servers Cause Cooling Issues

The good news is that servers are getting faster, smaller, and less expensive. The bad news is that low-end server technology is racing ahead of the ability of many data centers to keep the increasingly dense and fast systems cool. Experts say that users may have to invest in new cooling, monitoring and power equipment, or even retrofit their data centers or build new ones, to accommodate the servers.

Some users in the IT community are calling for manufacturers to shift from building denser systems to making ones that use less power. It is just a fact that faster and smaller servers run hotter. Data center personnel also point out the need for manufacturers to set up development partnerships with vendors of cooling and power protection products.

The overriding problem is that improper cooling can shorten a server's life or cause failure. IT departments are now faced with a situation where equipment that can use more power then ever before is delivered in a smaller footprint. Too often that means that the amount of power delivered and required exceeds current techniques for cooling data centers.

The next generation of blade servers will exacerbate the problem. Some analysts claim that blade servers are most likely going to be in just about everybody's data center sooner or later. Blade server racks come in a variety of sizes with different levels of power consumption. But they all need to be properly cooled, and that can be a problem for many data centers.

For their part, vendors say they are working to make systems more efficient but face a catch-22, with some users complaining about heat and others calling for more speed. They point out that adding cooling technologies to the server itself will come at a cost. A Dell spokesperson said that "if you introduce something besides traditional fans, heat sinks and airflows to a commodity server, that $2,000 server is not going to be $2,000 anymore." IBM is working on built-in cooling technologies that direct airflow and reduced the number of heat-generating fan motors. Liquid cooled systems may have to come into play at some point to assist the traditional fan systems.

To keep today's fast and dense servers from overheating, users have the following options:

Vendor Approaches

American Power Conversion has a closed, self-contained unit for supplying power and cooling.

Liebert Corp. offers cooling coils that are installed above server racks to draw heat out. Vendors are developing technologies for cooling the microprocessor itself. Some vendors also have introduced water-cooled racks.

User Approaches

- Limit the number of units installed in server racks.
- Reduce wire clutter under data center floors.
- Correctly position equipment to enhance cooling.

Affordable Network Management Tools

Network management tools often run tens of thousands - or even over $100,000 - which naturally is far out of the range of the vast majority of banks. But surprisingly, there are some excellent tools on the market for under $1000. All include simple monitoring tools such as ping and traceroute, but many include quite advanced features for under $500.

Nine packages that budget conscious banks may want to take a look at are: AdRem Software's NetCruch 3; Breakout Technologies' MonitorIT 6.0; ipMonitor Corp.'s eponymous product; Ipswitch's WhatsUp Small Business 2004; Neon Software's CyberGauge 6.0 and LANsurveyor 8.5; Nessoft's MultiPing 1.0 and PingPlotter 2.5 bundle; Quest Software's Big Brother; and SolarWinds.Net's Engineer's Edition Toolset 7.

All of these products have the expected status mechanisms, including notifications through e-mail, color statuses, triggered executables and audio cues. MonitorIT and ipMonitor especially excel in these basic notification functions. Perhaps the two most powerful programs are LANsurveyor and SolarWinds.Net's SolarWinds Engineer's Edition Toolset. Pricing is good too: If you don't need IDS scanning - a $295 option - you can get LANsurveyor for less than $500, with 20 systems agents included.

SolarWinds Engineer's Edition Toolset 7 runs $995 and includes 10 canned alerts that can be cloned and edited. This helps make alerting easy to setup. The Engineer's Toolset includes data-management capabilities, such as database backup and compression, and a host of other administrative controls.

Alerting in ipMonitor is strong as well, with 15 types of flexible alerts combined with good alert management. In addition to monitoring common TCP/IP services, ipMonitor monitors enterprise applications, including Active Directory, RADIUS and Lotus Notes. ipMonitor provides extensive systems management from a logically designed, snappy Web interface, plus it is fairly easy to install. ipMonitor 7.1, starts at $995 for 500 monitors; annual service included.

For cash strapped banks, Quest's Big Brother fits the bill - it is priced at the grand total of free! It is unusual for an enterprise-management vendor to give anything good away, but Quest Software does. Quest bought the venerable and free Big Brother network-monitoring application and now offers an enterprise version of Big Brother that adds support and advanced features.

Big Brother can monitor availability and utilization of CPUs, memory, disks, logs, systems processes, services and, of course, SNMP MIB variables. Configuration files control which processes the server runs, what devices are monitored and e-mail notification for alerts. The product's HTML interface is well-organized and uses the typical red for bad, green for good, yellow for warning. Like almost all of the programs, creating reports is simple and quick.

It is somewhat surprising that these applications can do a really good job of monitoring your bank's network for under $1000. Naturally, they will take time and effort to setup and configure, and some may require annual support and maintenance fees. But the ability to proactively manage your network should be worth the time, money and effort.

ATM Channel Undergoing Changes

MasterCard International has ordered all ATM switch providers to turn off machines not compliant with the new Triple DES encryption standards next April 1. Banks are also facing IBM's withdrawal of support for its OS/2 ATM operating system. Yet many financial institutions appear to be taking a fairly conservative approach to updating their ATM channel - boosting their normal attrition rates, but frequently opting for upgrades rather than brand new machines.

Perhaps it is a variation of the old saying "If it ain't broke, don't fix it," that can be paraphrased into "If it is compliant, don't fix it." If the machines work well and are compliant, many banks won't make the swap out even if it means passing up the ability to introduce personalized transactions, check imaging and other new, customer-friendly features that are available on newer machines.

Of course, very old units that are simply not capable of running Triple DES will have to be replaced. Another replacement scenario is where upgrades will cost almost as much as a new machine. Other FIs are looking to replace machines located in sites that generate the highest transaction volumes. The strategy is to maximize their investment by putting new machines -- and introducing new transactions -- where the most people would use them. Frequently, these new machines feature Windows-based operating systems and utilize TCP/IP communications.

The bottom line always comes into play: "will the new machines and functionality make me money or save me money?" Research shows that FIs are spending more now on their ATMs than they have in recent years, and they are purchasing machines with new technology platforms. The TowerGroup says that year-over-year ATM expenditures normally grow at a rate of 3 to 5 percent. However, because maintenance costs have remained stable, much of this spending is on new machines and software development.

Over 70 percent of ATM shipments by vendors serving the FI market in 2004 will go out loaded with Windows as the default operating system. That number has risen dramatically from 10 percent or so of ATMs shipped with Windows in 2001. By TowerGroup estimates, approximately 20 percent of the current global installed base is running Windows; by 2006, they expect that number will rise to 30 percent. Without a doubt, Windows, faster processors and IP communications are the springboards for offering new features at ATMs. Once fully compliant machines with these qualities are in the field, banks will be able to evaluate their options for adding new features and functionality.

The Downsides of Not Going Wireless

Most financial institutions are holding off on deploying wireless networks due to security concerns. Therefore, it may be quite surprising that according to the International Data Corporation, NOT introducing wireless technology may increase an organization's risk of security breaches. IDC research director Lars Vestergaard said interest in wireless technology by information technology managers is widespread but mild, with many using security concerns as a justification for not moving forward with a technology that has many benefits to the organization.

He feels that the largest security vulnerability is posed by rogue employees using wireless network cards without understanding the security, and thereby exposing the organization's network. IDC says organizations should make plans for incorporating wireless technology, which it says will inevitably become the standard. Vestergaard said his research has found interest by businesses in WLAN usage was quite extensive, but many IT managers are currently quite hesitant about adopting the technology. "Unfortunately IT managers are being uncertain about using this technology, but they use a lot of bad excuses," he said. "This is because they often fear a lack of security as well as an increase in transaction costs, for example, having to spend a lot of time and money on introducing the technology to new users."

He says that wireless networks can be properly encrypted and secured, even though there are conflicting standards and methodologies. He also claims "that IT managers are rejecting it on behalf of the company, but employees are still using the technology and that is not secure." The solution, according to IDC, is for IT departments to make strategies on how to deal with incorporating wireless technology.

USB Ports Represent Trouble

For the average corporate or home PC user, the initials "USB" refers to a computer port that makes it very easy to connect devices directly to a machine. With this connection, a person can transfer or copy information to and from a computer with little trouble.

But for security administrators and corporate executives, USB - short for Universal Serial Bus - is taking on an entirely new meaning: ultimate security breakdown.

Most organizations don't realize that USB and Firewire ports offer an unbelievably easy and accessible way to take sensitive information outside of the enterprise -

and this naiveté could cost them dearly.

If you look at the new corporate desktop releases from top makers Dell, Hewlett-Packard and Gateway, a single system can easily have up to eight USB ports. But it's not the sheer number of ports - it's the default plug-and-play configurations of operating systems like Microsoft Windows XP that are the real problem. Current operating systems provide seamless support for USB devices, and for good reason - their users want to be able to load photos, sync their PDAs and transfer music to and from their music players with no hassle. But the resulting security problems are significant.

For financial services firms, where sensitive information not only exists but is heavily regulated by privacy laws, there is monumental risk. So while FIs scramble to turn off the data spigot with no guarantee that software or PC manufacturers will do anything to stop default USB access, things are only going to get worse. Several trends will feed this security dilemma over the next 12 months, including:

- Music players such as Apple Computer's iPods, digital cameras, PDAs and other gadgets will continue to see rapid adoption among consumers and business users. With no configuration at all, an employee can plug a USB keychain with a gigabyte of storage into the back of a corporate PC. Employees already bring digital cameras to work to download photos to serve as desktop wallpaper or screensavers. These devices are normally plugged into home computers with a fraction of the security of today's enterprises, making it incredibly easy for someone, even unintentionally, to download a nasty virus or destructive code.
- Wireless LANs and laptop computers are the current hot vectors for malicious code infections, but the recent appearance of malicious code in portable and personal devices does not bode well for security administrators. Infected PDAs syncing to a corporate computer could result in a scenario where malicious code is passed from device to machine to corporate network. It's also conceivable that future malware will seek out portable media solely for the purpose of proliferation.
- The convergence of different computer components and technology could present the ultimate dilemma for security personnel. Mice, keyboards and other components that are intrinsic to everyday computing, combined with storage capabilities, are a potential Swiss Army knife for data thieves and insiders or yet another threat vector for malicious code exploits.

Unfortunately, most organizations are still drowning in their battle against malicious code and vulnerability patching, keeping the focus on perimeter security technologies, such as firewalls, server anti-virus strategies and content filtering at the gateway. While these measures are important and administrators must continue to lock things down at the network hub, the number of spokes is growing exponentially. Larger institutions have hundreds or thousands of machines hooked up to the network at any given time. When you factor in the possibility that very soon there could be multiple devices per PC with unlimited access, it presents a very sobering reality for the bank's security personnel.

"…most organizations are still drowning in their battle against malicious code and vulnerability patching…"

There are immediate steps that FIs can take that will go a long way toward solving this problem, including a "white list" approach to block unsanctioned devices, applications and executable files from all of their machines. Until these types of measures are implemented, USB devices will continue to be the weakness in perimeter security's Maginot Line, allowing a relatively easy and tempting way for wayward insiders and malicious code writers to hurt financial services firms.

A major step toward solving this problem will be turning their ultimate security breach into an unbreakable security barrier.

Thanks to Dennis Szerszen, vice president of business development at SecureWave for contributing this article. Dennis has over 20 years of product management, marketing and business development experience working for IBM where he was responsible for introducing new systems management and security software and services offerings. In recent years, Dennis directed Hurwitz Group's security practice where he had the opportunity to work with some of the most innovative and influential companies in the IT security and systems management markets. SecureWave, a maker of end-point security solutions, offers a line of Sanctuary products are based on the use of a white list to deliver an "inclusive" based security solution for businesses. Dennis can be reached at (919) 806-4410

Passwords and Biometrics

Passwords, the dominant form of securing an organization's assets, are a failure, according to a leading research firm. The Meta Group says that passwords' failings range from organizations wasting time creating convoluted policies to spending too little time protecting crucial applications. On the end-user front, meanwhile, passwords are ineffective when people have too many to maintain and tend to write down complex passwords. Many people are asking "After three or four decades, isn't there something else besides passwords?"

The solution that organizations are looking for is a low-cost way to add strong authentication to identity management. Some are trending towards the idea of some sort of supplement or alternative to passwords. Among the possible additions or alternatives to passwords are such concepts as: tokens, smart cards, fingerprint readers and PKI-style services. Tokens have been around for a long time, but unfortunately their price has not come down significantly. Currently, strong authentication schemes that use tokens - often USB-based devices that plug into the PC - cost too much, around $40 to $50 per user per year over a five-year period.

Smart cards are coming down in price, but still require a reader. However, a Silicon Valley company called OHVA says that they have inexpensive smart card technology right now. They claim that they can deliver a smart card-based system authentication system for just five dollars. That is the kind of price point that will make organizations take a second look. As for biometrics, the fingerprint readers certainly have not come down to that price level yet. But, as more and more manufacturers build the readers into their keyboards, mice and laptops, fingerprint biometrics should become much more appealing. As one analyst put it, "Passwords are just not cutting it, but until there is a very low-cost alternative this is all we've got."

Keep Your Security Efforts Visible

In some organizations, security spending is often an afterthought. Of course, experienced IT pros know that spending money up front on security can often save much more money in the long run. Budget decision makers need to see where security dollars are going, and they need to understand the impact of these funds on the operational health and safety of your network.

However, it can often take some extra effort to convince C-level executives and Board members that a proactive security strategy is a good investment. Budget decision makers need to see where security dollars are going, and they need to understand the impact of these funds on the operational health of your network and bank.

Some security analysts suggest creating a regular report to show senior management the return on investment for security spending. They recommend publicizing the positive and proactive impact of your security solutions, and create visibility for the IT Department and their security efforts.

A good place to begin is by calculating what it would cost to restore the most mission-critical servers and workstations on your network after a virus, malware or attack renders them useless. Increment that value for each new threat and attack that works its way onto your network.

One of the easiest ways to get the word out is via e-mail. You could use your security devices to generate reports, and create a daily or weekly summary of security events, then e-mail this report to appropriate staffers. This report should keep people informed of what the security administrator is doing and provide visibility of their positive contribution to network operations.

It is advisable to develop a specific report style, and stick to it. Keep your security reports simple; limit them to one page, and include links to in-depth background information for the headline topics on your report. Sending daily or weekly e-mail reports is a good start. However, it would be nice to establish a security Web page on your intranet and an internal security monitoring Web page for your bank.

Here are some security monitoring sites on the Web that can provide you with ideas for adding info to this intranet's content:

- Internet Storm Center: This is a good source for data to include on your page. The World Map section shows the top ports that people are actively scanning.

http://isc.sans.org/

- Internet Traffic Report: This site offers a health index that details speed and availability of backbone networks around the globe.

http://www.internettrafficreport.com/

- Symantec Security Response: You can customize a security alert box to feature live virus activity levels and reports of virus in the wild.

http://securityresponse.symantec.com/avcenter/

Most organizations look at network security spending as red ink on their budget. To show them otherwise, it helps to develop a method of showing the positive impact of security on your network. At the very least, your managers will feel better informed, and your users will gain an understanding of the work that goes into protecting the bank.

Hosted CRM Can Have Hidden Costs

Hosted CRM (Customer Relationship Management) systems are certainly far easier to deploy than in-house systems. They are also normally less expensive as well. However there can be significant hidden costs with the hosted or ASP (Application Service Provider) systems because every organization must pay the strategic costs of integration and customization - no matter if it is a premise-based or a hosted application.

Fortunately, hosted CRM vendors are working hard to ensure that their solutions make integration, configuration and customization easier than ever before. That said, it is important for users and potential users to understand that the total cost of ownership of these applications may be higher than they imagine. For instance, customization is still a cost outside of the monthly subscription rate. In many cases, CRM-deploying organizations wrongfully assume these costs will be less because the application itself is less expensive.

Other issues that banks looking to take the hosted CRM plunge need to look at are: software upgrades, bandwidth and hardware. Some users expect continual improvements in the software on a quarterly or at least six-month cycle, but vendors may not be so quick to update and enhance. Plus, what about the subscription price - will it go up when there are major upgrades? Bandwidth is always a concern when running any hosted application so be sure to test with the maximum number of concurrent licensed users at the same time to make certain that everyone is getting good response times. Finally, perform due diligence on the vendor's data center hardware so that you feel comfortable with their capacity, redundancy, security, etc.

As the CRM ASPs become more popular and sophisticated, users tend to expect them to perform at a level comparable to enterprise and core system software. Downtime is not acceptable, and some ASPs, such as NetSuite, have begun marketing themselves with guaranteed levels of performance. Yet, it may not be realistic to expect them to perform at this level since many of them are quite young companies. Service levels should be set in Service Level Agreements with financial penalties for not meeting set goals. As can be seen, an outsourced CRM solution - like any outsourcing - agreement must be carefully monitored and managed to remain effective and affordable.

New VoIP Phone Systems

We recently covered Cisco's remarkable success stories rolling out VoIP (Voice over Internet Protocol) systems, but 3Com and Toshiba are two competitors that also offer powerful VoIP systems. All three companies are in a dogfight for the burgeoning VoIP marketplace.

3Com announced an upgrade to its VCX enterprise IP PBX platform at the Fall Internet Telephony Expo in Los Angeles. This solution adds remote-site failover and survivability features in case of network or IP PBX equipment failure. Also, 3Com says its new bundle of convergence applications based on the Session Initiation Protocol (SIP), including unified messaging, presence and multimedia conferencing, can help individual employees work more efficiently.

3Com launched Version 5.0 of its SIP-based VCX call control software, which runs on its VCX 7000 IP PBX hardware platform. The new software now runs on the Linux operating system and Sun's Solaris, which gives users the option of using an Intel-based server as an IP PBX, in addition to Sun's proprietary server platform.

VCX 5.0 also includes a feature called Voice Boundary Routing, which lets IP phones distributed across a WAN (wide area network) switch over to a back-up VCX in case of a primary call server failure. When deployed with VCX 3000 gateways in a branch office, Voice Boundary Routing also lets IP phones in that office make calls through the local public switched telephone network in case the primary WAN link fails. This feature should bring a great deal of peace of mind to organizations that demand no down time from their phone system.

3Com claims that their Voice Boundary Routing is better than competitive technologies such as Cisco's Survivable Remote Site Telephony, because other VoIP survivability technologies only provide basic local call features to phones when a WAN link goes down. Voice Boundary Routing lets local gateways provide all VCX call features, a local-branch version of voice mail and other applications.

3Com also is introducing its Convergence Application Suite, which includes software modules that allow for SIP-based messaging, presence and conferencing applications for VCX 7000 systems that run the 5.0 software. The new 3Com VCX 5.0 and conferencing applications range from $70 to $200 per user. A VCX 7000 with the 5.0 software costs about $500 per line, not including IP phone costs.

While 3Com goes after large businesses, Toshiba is targeting shops with fewer than 200 users with its latest Strata CIX offering. Their system is a dual-processor IP PBX that can handle SIP- and Media Gateway Control Protocol (MGCP)-based IP endpoints, and legacy digital phones that worked with Toshiba's old key telephone systems.

Along with this new platform, Toshiba also is introducing its Strata Media Application Server (MAS). This Windows-based server supports the vendor's new FeatureFlex applications, which include SIP-based presence management and conferencing, and call routing and screening features.

Toshiba makes a line of IP phones that use the MGCP VoIP protocol and support the full set of features and functions on the Strata CIX. Third-party SIP phones will work with the Strata CIX, but more advanced features such as presence and caller ID are not supported. All features are supported on Toshiba digital handsets attached to a Strata CIX. The Toshiba Strata CIX costs about $500 per line not including phones. Look for prices on all vendors' systems to come down rapidly as VoIP gains more widespread acceptance.

Voice-prompted Banking Gains Momentum

Voice-prompted banking has been fairly slow to gain momentum because for many years it was poorly applied, prone to inaccuracies and easily confused - by background noise, for example. Automated touchtone phone systems have typically been the link between the public and the call center. But several industry experts say the familiar touchtone systems may soon go the way of the rotary phone.

Proponents declare that the troubled days of voice systems are in the past and that there are significant advantages to voice-based technology over old fashioned touch tone prompts. They argue that in order to improve client service, banks must turn to speech-based technology because it can really enhance their service levels.

A high quality voice-enabled automated call system determines clients' needs through voice prompts and quickly routes calls to the appropriate personnel. The system lets callers skip many of the prompts they typically encounter with a touchtone system before getting to the point where they need to be. A voice-based solution helps callers complete their business faster, which in turn increases client satisfaction.

New Speech Patterns

Research firm Datamonitor predicts that FIs will soon begin relying on speech technology for more than call steering, allowing customers to access accounts, transfer funds, pay bills and more. The first step is routing, the follow on steps are empowering a customer to be able to do on the phone, what they can do on the Web. Additionally, Datamonitor analysts think that another trend will be to utilize biometric voice prints as a secure means for accessing accounts. This will increase call convenience, but they note that the technology must gain a proven track record before FIs will rely upon it for identification purposes.

While its potential in other areas remains largely untapped, the primary benefit speech technology offers banks today is improved customer service. It provides customers with greater interaction and ease of use. For example, speech systems don't require people to spell names on the touchtone pad. Callers can interact directly with the interface in their own vocabulary and at their own pace. Voice-based technology can also mean cost savings for the bank by freeing employees from routine matters and, by shortening calls which saves money on 800-number line charges.

Closing the Generation Gap

Vendors and FIs have learned quite a bit from the first generation systems. For instance, early systems tended to ask much too generic questions such as "What would you like to do?" That was too open-ended, with too many potential answers. Today's systems limit potential answers by asking more specific questions, or Yes or No questions. Other recent improvements include increased computing speeds, complex algorithms used for improved speech recognition and more.

Current technology keeps behavior in mind, too, not just literal speech. For example, if a caller wants the second of four listed options, she will likely interrupt the menu after the second item. Even if the system doesn't recognize exactly what the caller says, it can assume the person wants the second item, because that is when she spoke.

Banks need to ask important questions long before they implement a system. Why are customers calling? What do they need? How can a voice-enabled automated phone system be designed to perform necessary tasks efficiently enough to prevent the customer from abandoning the call out of frustration? Any successful system must be built with the answers to these questions in mind.

As voice recognition technology advances, it will soon be able to keep pace with humans and omit things such as coughs and sneezes. In the meantime, there are still some issues with noise, dialect and customer comfort levels. The keys to rolling out a successful system are to test the vendor's solution thoroughly, approach the implementation from the customers' point of view and constantly monitor the live system.

Establishing a Sales to Service Program

Is your bank having a hard time getting your call center staff to recommend upgraded products and services during inbound calls? Are they tentative about placing outbound calls? Perhaps most of your Customer Service Representatives (CSRs) were originally hired and trained to focus on service, not sales. How can you help transition them from service to sales? Naturally, training is key to the success of this program and some investment is required to get the results you want.

Some sales experts and consultants suggest setting up a Service to Sales Program. The idea behind this program would be to focus on your existing customers and establish or re-kindle your relationships with them. Some plans include scheduling inbound CSRs to make outbound calls during slow and evening times to "manage accounts." They see this as a very "soft sell, touching base" approach. It can also be used with new customers to follow-up to make sure that they have received their checks, debit cards, etc and to make sure that they had a good account opening experience.

Outbound sales proponents tout the following benefits to call center employees:

- The additional function adds variety to their workday.
- The introduction of ways to increase their incomes will get the attention of service staff.
- Completing additional training is always a great benefit to add to resumes and is a career development opportunity.

The first step for the staff will be to go through sales training before they begin this endeavor. Your bank will want to work with a firm that has a great deal of experience in regards to telemarketing and sales coaching, especially in regards to financial services products. Coordination will be needed with the Marketing Department as well in regards to their current promotions and overall business goals.

Once you have developed your plan, here are some key points you should make sure are included in your training:

- This is not cold calling. This is customer relationship management, so think both long and short term.
- Ask questions to define customer needs. Customers will buy only when they perceive a need.
- Recognize the need to use good listening, questioning and interpersonal skills.
- Recognize that upgrading can benefit the customer, the employee and the bank.
- Listen for upgrade opportunities and learn how to identify buying signals.
- Know how to ask for and close the sale.
- Everyone cannot know everything about everything, so learn the best way to "hand off" and

not lose the sale.

- Learn how to set goals that will result in both sales and service success.
- Celebrate success and have fun.

Of course, this training can benefit others in the bank besides inbound and outbound call center personnel: tellers, loan officers and other front line employees should go through it too. Establishing a sales culture at your bank is a long term and never ending project, but one that can reap huge dividends for the bank.

Measuring Call Quality

Traditionally, call centers have measured call length and the number of calls as indicators of how the center is doing. This approach is rather outdated and really is no longer sufficient. Quality, rather than quantity, has become the key element in identifying call center success, and caller satisfaction in particular. Automated quality monitoring systems provide insights into call center quality and productivity and help to optimize CSR performance.

Quality monitoring systems can consist of a simple tape recorder all the way up to client/server-based network recording systems. The higher end solutions often include training modules for CSRs, caller survey tools and screen capture software. Some systems even have "call mining" software that identifies recordings containing certain words or phrases, or that detects stress in an CSR's or caller's voice.

The basic three components of quality monitoring include:

- Listening to the call via voice and data recording;
- Evaluating CSRs through software that takes the bias out of the process; and
- Reporting capabilities to analyze and track the evaluation data.

But these basics are just the bare bones starting point — quite a few vendors also offer CTI or computer telephony integration interfaces; e-learning capabilities; agent evaluation software; analytical and reporting applications; screen capture to record both voice and data activities; and multimedia recording of voice, e-mail, and Web chat.

Yet most call centers are still focusing on call logging. Research shows that the call center recording market is dominated (80%) by call logging, with quality monitoring systems still in the minority. Banks looking to take the VoIP (Voice over Internet Protocol) plunge and want call recording will have to make sure that the voice/data recording system they use works with their IP switches and infrastructure. Several vendors, including Nice, Witness Systems, etalk, and others have IP offerings for the monitoring and recording products.

Two other call recording trends are screen capture and e-learning. High end voice/data monitoring systems enable supervisors to get insight into how effectively CSRs are handling screen navigation and responding to customer needs. Because an automated quality monitoring system records both the voice conversation and the CSR's data screens, supervisors can actually see and hear what happened between the caller and CSR.

As for e-learning, contact center managers are beginning to use it to deliver and reinforce training. In today's hyper-competitive financial services marketplace, it is more critical than ever to have proficient and well-trained CSRs. Recording and analysis software provides banks with the information needed to make changes, identify training needs and coach CSRs to ensure the most effective and efficient customer interaction.

Proponents of these systems believe that through monitoring, evaluation and integrated e-learning, call centers can help ensure their callers interact with enthusiastic, motivated CSRs and obtain consistent service via Web, e-mail or the telephone. While not inexpensive, these systems should provide a good payback with increased customer loyalty and satisfaction.

Microsoft Moves to Monthly Patch Cycle

It has been one year since Microsoft moved to a monthly patch release cycle. Has this once a month schedule been helpful or hurtful for harried network administrators? Many IT managers believe that Microsoft's move to a monthly patch-release cycle has made it easier to install security updates for Windows and other products, even as they were greeted with a barrage of new fixes, many for flaws that were given *"critical" severity ratings by Microsoft.*

The October patch rollout was one of Microsoft's largest yet this year, consisting of 10 separate patches designed to address a total of 20 vulnerabilities across a wide range of the company's software. Seven of the security updates were rated as "critical" for users to install, and the other three were labeled "important."

The massive release highlighted Microsoft's continuing struggles with software security. Nevertheless, many in the industry think that the monthly cycle that the vendor has followed for almost all the patches released since last October has made the patching process more predictable and manageable. They find it helpful for planning purposes and in allowing them to evaluate the patches once a month, versus having them trickle in randomly throughout the day, week and month.

Others say that Microsoft appears to have become much more aware of the heavy burden that patching systems put on IT managers. A regular patching schedule can reduce much of the instability that results from intermittent releases and helps ease the challenge of keeping up to date on patches. A spokesperson at Microsoft's Security Response Center, said the shift from an ad hoc patch release process to a weekly schedule and then to the monthly one was driven by feedback from users who said they "were not able to plan well because they didn't know in advance when we would have patches for them."

The policy of releasing patches on the second Tuesday of each month has also given the software giant more time to work on improving the quality of its fixes and to do a deeper level of testing in the patch development stage. However the schedule does have detractors who say that a monthly schedule can sometimes expose users to longer periods of risk. They point out the worst case scenario: If a new security flaw is discovered right after an update, you will have to wait 30 days for a patch. Some also argue that grouping together multiple security fixes in large patches can increase the testing burden for IT managers.

In response to concerns about users being exposed to longer periods of risk, Microsoft noted that they will issue out-of-cycle fixes if the situation warrants it. In late July, for instance, the company rushed out a patch after an active exploit was found to be taking advantage of a flaw in Internet Explorer. Overall, it appears that the monthly patch cycle should make it easier for busy bank network admins to maintain more control over the never ending patch process.

Disabling Internet Explorer

Internet Explorer users have witnessed a rash of IE exploits and fixes released in the last several months. The U.S. Computer Emergency Readiness Team (US-CERT) even recommends using a different browser. But if some employees don't need access to the Internet, it may just be easier to disable or remove Internet Explorer.

If you are running Windows 2000 or XP, there is good news and bad news. The bad news is that you can't remove IE without crippling your operating system. However, the good news is that you can fairly easily disable IE for your users.

Several simple, popular methods exist to disable IE. Perhaps the easiest way to remove users' ability to browse with IE is to add a bogus proxy server to IE's Internet Settings.

Follow these steps:

1. In IE, go to Tools | Internet Options.
2. On the Connections tab, click the LAN Settings button.
3. In the resulting dialog box, select the following check box in the Proxy Server section: Use a Proxy Server For Your LAN (These Settings Will Not Apply To Dial-up Or VPN Connections).
4. Enter 0.0.0.0 in the Address text box.
5. Enter 80 in the Port text box, and click OK.

Or you can also restrict Internet settings via Group Policy. Follow these steps:

1. On your domain controller, right-click the organizational unit that contains your domain users, and select Properties.
2. On the Group Policy tab, click Edit.
3. Expand User Configuration to set restrictions on a per-user basis.
4. Expand Windows Settings, and expand Internet Explorer Maintenance.
5. Select Connection, and double-click Proxy Settings.
6. Select the Enable Proxy Settings check box, add 0.0.0.0 to the HTTP entry, and click OK.
7. Expand Administrative Templates, and expand Windows Components.

8. Select Internet Explorer, and double-click Disable Changing Proxy Settings.

9. Select Enabled, and click OK.

Remember that Enabled sets a restriction, Disabled prevents a restriction from applying to a group of users (even if you enable it for a broader category of users), and Not Configured doesn't set the restriction. Note that adding a bogus proxy server to your Internet settings won't affect Automatic Windows Update from connecting and updating your operating system.

No matter how many patches Microsoft releases, ActiveX and the Browser Helper Object (a file loaded with Internet Explorer) are all an attacker needs to control your system and steal your data. Microsoft designed IE for functionality - not security. And antivirus software can't defend your network against IE exploits.

Windows security isn't about eliminating security holes; it is about managing risk and user functionality. All operating systems have vulnerabilities, but Windows' popularity makes it the target of choice for most black hats.

Getting Control of IM

While company attitudes toward instant messaging (IM) vary, most IT managers are being forced to face up to a simple fact: IM, a technology that started as a consumer toy, has not only worked its way into common use in many companies but is also increasingly being used for serious business communications. As a result, like it or not, IT managers need to get serious about controlling IM. That means creating and enforcing rules about how IM is to be used and for what purposes. It also means making IM more secure and trackable than current, consumer-oriented services such as AOL's Instant Messenger or MSN Messenger.

One company that is working with financial institutions is FaceTime Communications. Their IM Auditor software is used to track and inventory messages. The consumer IM services lack the kind of security usually demanded by enterprise users and provide no ability to archive and index messages. That is why some organizations are turning to IM products tailored for enterprise users from vendors such as Ikimbo, WiredRed Software, NetLert Communications, FaceTime and Lotus Development Corp. Such products solve some of consumer IM's security problems by moving the IM server inside the enterprise firewall and keeping IM messages off the public Internet. Most add encryption; some also add administrative features such as the archiving and indexing of messages.

What makes consumer IM services inherently insecure? Unfortunately, lots of things. First, consumer IM products, once activated on a user's desktop, open a channel through the firewall that can easily be exploited by hackers. That is particularly true because IM services, rather than consistently using the same server port, tend to scan firewalls for available ports. That makes it difficult to use virus-scanning tools to clean IM traffic or attachments. Another security problem intrinsic to consumer-grade IM applications is that content is typically unencrypted.

It is obvious that any bank that wants to let their employees use IM needs to control it and administer it in a properly secure manner. Although behind-the-firewall, enterprise IM products offer enhanced security and the ability to allow instant messages to be audited, many come with a drawback: since they require proprietary clients and run over private networks, they are not easily open and available to all users. However, some enterprise IM vendors have engineered a way around that limitation. Omniprise, for example, an enterprise IM product from Ikimbo, includes a client that can be downloaded onto invited parties' computers. An administrator keeps control of who gets invited to participate. This allows the IM network of users to expand while keeping sensitive information out of the wrong hands.

How to Decide

So how should IT managers decide whether to standardize on an enterprise IM product, ban consumer IM altogether or take a wait-and-see approach to IM? bank network admins should first determine how much IM is being used already in their bank and what percentage of it is on consumer IM platforms. It is fact that very few organizations know how much IM is being used, so research is the first step. If the employees are using it, there is a high probability that they are using a consumer-grade service - not a good scenario. The next step would be to make a business case for installing a secure IM package and consider blocking the commercial IM communications.

Finally, experts say, IT managers should set IM usage policies. For example, a consistent IM user-naming convention similar to that which most organizations have put in place for e-mail should be created to ensure that your IM doesn't degenerate into arcane and subjective naming schemes. IM is here and will continue to grow, so banks will need to get onboard with this new generation of secure platform.

PSTN vs. VoIP

Many people are confused - and understandably so - over the relationship between the public-switched telephone network (PSTN) and Voice over Internet Protocol (VoIP). It is always good to get back to a few basics about the relationship between the public-switched telephone network and Voice over IP.

The PSTN includes a signaling system, a series of central offices and a distribution network. The PSTN employs a packet-based network called Signaling System 7 (SS7) or Common

Channel Signaling System 7 (CCSS7) to determine the best call route, connect the callers and control calls. Private voice network systems like PBX and key systems work with the PSTN to create a hybrid public/private network.

Using IP to signal and transport voice brings several fundamental shifts to traditional voice communications. In the legacy PSTN environment, unused bandwidth cannot be shared; using packetized transmission (like an IP packet) for voice shares unused bandwidth and allows for greater efficiency, thereby reducing cost. IP is the packet protocol of choice for voice because the overall volume of users' WAN (wide area network) traffic is dominated by IP.

In the PSTN, voice network features are delivered to a user on a static pair of copper wires to a static local central office switch or PBX. VoIP allows the traditionally switched services to be delivered to a user anywhere the user is connected.

Deploying VoIP

The three most common ways to deploy private VoIP include the use of VoIP gateways, VoIP-enabled routers or an IP-PBX. VoIP gateways represent one of the easiest ways to deploy VoIP. A gateway transforms SS7 signaling and traditional voice transmissions into IP-based signaling and transmission techniques. By installing a gateway, a business can connect to an IP or other data network and a TDM (time division multiplexing) network simultaneously.

VoIP-enabling routers means adding a gateway function to a router. Routers can be upgraded to include the gateway and voice-specific features. IP-PBX and IP-enabled PBX deployments are similar in that they start with PBX features and include a gateway function.

Some telecom experts believe that the faithful PSTN is on its last legs. They point to recent news from AT&T (along with announcements from Verizon and Sprint Canada) as marking the official beginning of the end of this venerable stalwart of the telecom infrastructure. Mainstream carriers not only are announcing intentions to embrace new VoIP technologies (not long ago the exclusive province of entrepreneurial upstarts), they are practically stumbling over each other in a race to roll out IP-based network infrastructures that are less expensive to build, deploy and maintain.

As long as the quality of these services can approximate that of the PSTN dial-tone, then everybody theoretically wins: carriers reduce their costs and should be able to cut their prices to consumers with no reduction in the user experience. As an added bonus service providers reap higher profits. It should all just be a matter of time before this transformation from PSTN to VoIP is complete.

Protecting POS Terminals from Virus Threat

VeriFone and McAfee announced they would jointly develop an antivirus solution for Internet-enabled payment terminals at the point of sale. This is a preventative measure to guarantee the protection of transaction data from malicious software as merchants employ IP-enabled card swipe devices.

Viruses and worms cost U.S. businesses billions of dollars yearly. Lately, there has been an amplified consciousness of the threat to payment devices that transport and encrypt confidential consumer data.

"With the growth in Internet Protocol-enabled payment devices, we want to provide merchants with assurance transaction data will be safe from increasingly sophisticated malicious software," says

Paul Rasori, vice president of product marketing for VeriFone. "VeriFone aims to provide the highest-levels of security and our IP-enabled terminals have operated without intrusions. But we are determined to improve the security in our solutions by teaming with the industry leader in network and Internet security systems to preempt the threat of malicious software."

The two companies will develop software for real-time monitoring and attack pattern update services using McAfee VirusScan for VeriFone IP-enabled payment devices, including those already installed in the field. VeriFone, which already supports Ethernet, Wi-Fi, 2.5G and 3G wireless IP networks in POS products, will work with credit card processors and independent sales organizations to activate and support the antivirus protection solution at the merchant level. The companies expect to make the antivirus solution available initially in North America beginning in early 2005.

"Online offenders are always on the lookout for new opportunities to spread malicious threats, so we must always be a step ahead of them," states Bill Kerrigan, senior vice president of McAfee Consumer. "By developing an anti-virus solution for the POS space, we are responding to an unfilled need in the marketplace, while also providing a high level of security to consumers and merchants."

Credit and debit charges now account for almost a third of total personal consumer expenditures in the U.S., resulting in a heightened risk of wide scale virus assault on point-of-sale payment terminals could be devastating for impacted merchants.

BANK *tech-trends*

Financial Technology News & Strategies

UPCOMING WEBINARs

Catch Them If You Can! IT Fraud Prevention

From spoofing to phishing, fraudsters are increasingly using the Internet to cheat your bank and your customers out of money and confidential information. In this 45-minute webcast, we'll equip you to spot IT fraud - and stop it before it compromises your assets.

Here's what you'll learn:

- ✓ How to identify the most common methods of IT fraud
- ✓ What trends indicate about upcoming threats to financial organizations - and how to guard yourself against them
- ✓ How to use employee training to protect your bank from fraudulent Internet and e-mail scams
- ✓ Where to go for the resources and tools you need to protect your bank's assets

Who Should Attend: CEOs, Audit/Compliance Personnel, IT Managers, Networking Staff.

Presented by: SecureWorks

Date: Thursday, December 16, 2004 1:00PM Central (2:00PM Eastern, Noon Mountain, 11AM Pacific)

Costs: Free

Register Now: http://www.secureworks.com/seminar/Dec16Webcast.html

BANK *tech-trends* Order Form

YES - Start my subscription to BANK *tech-trends*

❐ Enclosed is a check* for $99

* Payable to BANK *tech-trends*

❐ Bill my firm

For Faster Service
Go To Our Website:
http://www.banktt.co

Name: ______________________________

Position: ______________________________

Institution: ______________________________

Address: ______________________________

City/State/Zip: ______________________________

Phone: ____________ Fax: ____________

Email: ______________________________

Thomas Wright
Publisher
9510 Baltimore
Overland, MO 63114
314-428-5005
email: tom@banktt.com

Roy W. Urrico
Editor
518-793-0550
email: roy@banktt.com