A ROYAL MEDIA GROUP PUBLICATION

MAY 26, 2003 VOL. 1, NO. 2

BANKSECURITYNEWS

INSIGHTS ON CORPORATE AND INFORMATION SECURITY

WWW.BANKSECURITYNEWS.COM

NEWS INSIDE

Bank Security News is published by Royal Media Group
1359 Broadway
Suite 1512
New York, NY 10018
www.banksecuritynews.com

ISSN 1098-8335

"SILENT" ATTACKS PROMPT BANKS TO RESTRICT NETWORK ACCESS, RAMP UP SECURITY

Banks are reporting an increase in so-called "silent threats" — system intrusions that occur as employees or hackers with access to corporate servers make organized attempts to enter these servers to gain access to sensitive customer information or data.

Silent threats are most often perpetrated by employees, many of whom are being granted wider access to operating systems and various servers through virtual private networks. But, it also occurs when non-employees gain access to servers via employees' lost or stolen cell phones or laptops or Blackberries or other personal digital assistants.

"Silent threats are a major issue that we deal with as we add new points of presence into our operating environment," said **Jim Wade**, senior vice president and chief information security officer of Cleveland-based **KeyCorp**.

In fact, Wade said an estimated 80% of all hacker attacks are internal and come from people who have authorized access to servers.

The chief challenge in monitoring and managing these threats is that unlike hackers or viruses, they are less publicized, and are more difficult to manage and predict, much like employee misbehavior in general, said **Ken Barney** of Plano, Texas-based **EDS**, a leading global technology IT services vendor, whose clients have seen a spike in silent threats.

"The question for IT officers becomes, 'How do you watch over your own people, your own vendors?'" Barney said.

Continued on page 8

PEOPLE SCAN

- **Valorie Kacherian** takes post at **Fairbanks Capital**
- **Raymond Touma** joins **Provident Bank**'s IT group
- **Joan Guggenheimer** named **Bank One**'s chief legal officer

See page 9

COSTS FOR PATRIOT ACT COMPLIANCE JUMPING AT E-FUNDS, PNC, WELLS

Several of the nation's largest financial institutions, including **e-Funds**, **Wells Fargo & Co.**, and **PNC Bank**, are starting to incur greater expenses in areas such as staffing and training as they struggle to abide by tighter customer identification rules under the Patriot Act.

"The reallocation of resources is going to be a major challenge for all financial institutions," said **Ted DeZabala**, partner and leader of security services group at **Deloitte & Touche**. "There's no way around that."

Patriot Act-related software costs for banks have already been documented, and they won't be cheap. For a bank the size of **Citigroup**, the cost of software to handle Patriot Act compliance is estimated to be about $30 million. And software that helps banks determine who their customers are, tracks their funds and normal transaction activity under the "Know Your Customer" provision of the Patriot Act can range from $1,000 for a small community bank to $150 million to $650 million for larger institutions, according to **TowerGroup**, the Needham, Mass., consultancy.

But it is in staff deployment, training, and maintaining customer trust that costs are ballooning higher than expected at e-Funds, PNC, and Wells Fargo — and many others — although each declined to give specific dollar figures.

The Patriot Act requires banks to ask for additional information from customers deemed to be "risky." The riskier a person appears, from a criminal standpoint, the more diligence expected. Yet, smaller banks may have a harder time conducting such due diligence than larger institutions, said

Continued on page 6

Q&A

JIM WADE, SVP & INFORMATION SECURITY OFFICER, KEYCORP

BANK ONE SETS UP ITS TOWER

Bank One Corp. has purchased consoles from Middle Atlantic Products to house the surveillance and monitoring hardware at its 48-story BankOne Tower in Indianapolis, *Access Control & Security Systems* reported. Financial terms of the purchase were not disclosed. The consoles retail for about $1,300 each. Bank One is based in Chicago.

For more information, visit http://www.middleatlantic.com/index.htm.

BANKS MUST ADD SECURITY TO RISK ESTIMATES, KEYCORP'S WADE SAYS

KeyCorp ranks among the nation's top super-regional banks, so corporate and IT security is anything but an afterthought at the Cleveland-based financial institution. That's not to say the nation's other mega banks don't have comprehensive security protocols. But how does KeyCorp's view of financial services security differ from other banks'? *Bank Security News* talked with **Jim Wade**, senior vice president and chief information security officer at KeyCorp, for the bank's perspective on security demands today – and how it expects those demands will change in the future.

BANK SECURITY NEWS: *What are the critical security concerns banks face?*

JIM WADE: In the past, banks were entrusted with information about their customers and clients. Now, with the interest in privacy and protecting the confidential information of clients, there's a great amount of pressure to do the right thing. Because the government is stepping in even more than the past because of terrorist concerns, we have to do a much better job protecting the information we have. There's a bit of opposition between security and confidentiality and the compliance requirements needed to make sure we're completely functioning in today's environment.

> "We look at each transaction and make decisions based on each one and add a compensating control to mitigate the risk."

BSN: *How is your company providing optimal protection against system attacks and in what areas do you feel its security could be enhanced?*

JW: I think it's key for us to blend the perspectives of all the various risk elements — operational, security, technology and business — into a completely integrated picture so that we can share alternatives with management. For example, if risk management only factors in security at the exclusion of all else, it doesn't give them a true choice of how to run the business. The challenge for us today is for senior people to not simply be proponents of their own areas, but [to] seek the consolidation of all the other risks in the area so management sees the big picture.

Even though we want to say we're mature in the practice, we may not be as good as we are. Generally, legislators do not weigh in on the things we do well. At least it may bring us to a best-practices approach.

BSN: *Will enhanced Patriot Act regulations force Key to use third-party software?*

JW: I am not sure we know the answer to that yet, given the newness of that legislation. Right now, we are doing most of it ourselves. That is not to say that as we move downstream, and legislators have us do more than we can do within our own facilities that we will not have to go to a software provider. From our perspective, we try to respond within our own capabilities.

BSN: *What protocols should be implemented to enhance XML's level of security?*

JW: Unfortunately, when XML was developed, it did not factor in security as one of its main focus points, so that there are some emerging standards that will need to be incorporated into the future. We are discussing ways to place it so that it ensures security. SXML may be one of the standards to use. Obviously, until that happens, we have to put in compensating controls in the web environment.

Many banks are addressing the lack of security as a risk-based approach, but all web-based transactions are not the same. We look at each transaction and make decisions based on each one and add a compensating control to mitigate the risk. For example, if a customer comes in simply to check the interest accruing on a CD vs. someone who is conducting a transfer via the internet, there are two opposite risks. For the first person you may simply do the standard

Continued on page 3

Response

HOW TO CONDUCT A "FORENSICS" INVESTIGATION

Hackers into bank computer systems are getting more sophisticated, and that is putting more pressure on the bank "forensics" teams that conduct investigations into wrongdoing.

Each bank conducts forensic investigations in different ways, and the ways in which they are toughening up their approaches to investigations also differs. Here's how **Network Intelligence**, the Walpole, Mass., maker of investigation systems, suggests banks conduct forensic investigations into system breaches:

• Search for the systems that have been compromised, discover the scope of the possible loss, and track backwards to discover where the first penetration occurred.

• Look at the systems that had the highest value data on them and look at configuration changes.

• Store logs of computer activity, since each hacker leaves a footprint. Ensure that the data pulled through computer forensics is actually raw data by storing the log on remote systems and making sure the data is secured through encryption. If the logs are modified, there is a chance they cannot be used in a criminal trial.

• Store and secure the data for extended periods of time. Often, a financial institution does not know it has been hacked until a month after the fact. A recent recommendation by the **Office of the Controller of the Currency** suggests that data be keyed for two exam cycles or a three-year period, which enables investigators to examine trends that may have developed.

KEYCORP'S JIM WADE

continued from page 2

user ID, password, PIN to authenticate the customer, whereas with the person coming across the web to do the transfer because the information is so sensitive, you may use SSL or encryption. If we are dealing with enough money, we will do multifactor authentication with smart cards, tokens, and biometrics.

BSN: *How do you handle "silent threats"?*

JW: We ask who our clients and strategic partners are, look at the information, and for assurance that they are going to protect the information at the same level, we require it to be protected within our operations. If we don't have that assurance, we add in compensating controls. Some of the controls are contractual as well as technological. In some cases, we sign off liability through contractual relationships or by using technology like access controls and firewalls.

We also require managers to validate the access that an employee, consultant or contractor has to our systems. Long-time employees may have several different jobs, with different levels of access to various areas of the banks. We periodically validate their access. Sometimes, I'll have to restrict what our clients or employees can do. But some executives have demands for access that go beyond what we might be comfortable with. So we have to measure that risk, and often add in additional technology like the procurement of software or ongoing maintenance.

BSN: *How far have banks come in computer forensics?*

JW: Forensics has become very sophisticated. We can now identify malicious wrongdoing ranging from people that are just doing something against policy, to those that are engaging in criminal activity. I think we clearly want to educate our employees that they should not have the expectation of privacy. Computers belong to the bank and, as a result, when someone is terminated and says, "I had a file on that computer about my PTA," that person should not expect that the company owes them those files. One of our chief considerations is whether we can conduct the level of investigations required to gather evidence, while minimizing damage and allowing users to continue their work. If you're truly trying to gather evidence that is going to be used in court, you need to have the ability to account for who was doing what, where and why. Most of the time we take systems offline and take a snapshot. If it's an investigation where you have to interrupt the system, you hope you've done the right job in having a back-up system to take its place.

REG FIRMS ISSUE GUIDANCE ON WEBLINKING

Concern about web linking between financial services companies has led four regulatory organizations to jointly issue their first guidance on the issue.

The **OCC**, **FDIC**, **National Credit Union Administration**, and **OTS** advised financial organizations last month to use clear and conspicuous disclosures to customers regarding their involvement in third party-supplied products and services, as well as implement programs that address customer complaints. Banks also were advised to check out potential web linking organizations and their activities.

Some security experts have grown increasingly wary of web linking as a security threat. Recently, **Bank of America Corp.** fell prey to a group of hackers who created a mirror site to www.bankofamerica.com and steered unwitting consumers to the faux BofA site.

For more information of the regulators' linking policies, visit http://www.fdic.gov/news/news/financial/2003/index.html or call Jeffrey M. Kopchik, and FDIC senior policy analyst, at 202-898-3872.

PEOPLE, ENTITIES MARKED AS INVOLVED IN DRUG DEALING

The Treasury Department's office of Foreign Assets Control (OFAC) publishes a list of individuals and entities that it considers Specially Designated Narcotics Traffickers, or SDNTs, with whom the federal government forbids dealings by financial institutions. SDNTs added in May 2003:

ORIGIN: MIAMI

Vidal Caggigas, Rolando; Passport No. 16822748

ORIGIN: Virginia Gardens, Fla.

Transporting LLC; Business Registration Document No. L00000012836

ORIGIN: WESTON, Fla.

Sepulveda-Iragorri, Inc.; Business Registration Document No. P00000115667

ORIGIN: NASSAU, Bahamas

Ardila-Marmolejo Ltd.; Business Registration No. 88,046 B

ORIGIN: CALI, Colombia

Sepulveda-Iragorri, Ltd.; No. n/a

The Treasury Department's OFAC also publishes a list of Specially Designated Global Terrorists, or SDGTs, with whom the federal government forbids dealings by financial institutions. SDGTs added in May 2003:

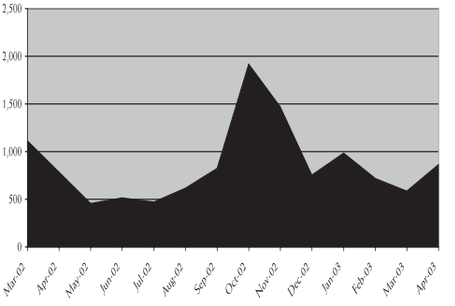
Batasuna*

Euskal Herritarrok*

Herri Batasuna*

Entry also known as Basque Fatherland and Liberty

VIRUS & WORM TALLY*



Source: Central Command Inc., www.centralcommand.com

*Reflects the number of worms, viruses, and "other malicious applications" for which Central Command updated its anti-virus software during a given month.

THE 10 MOST COMMON VIRUSES

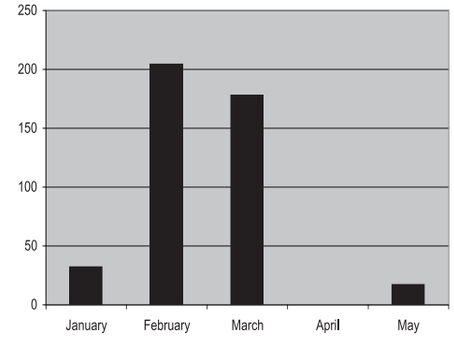
Viruses	% of Total, 4/03	% of Total, 4/02
Worm/Klez.E	18.7	79.2
Worm/Yaha.E	8.9	--
Worm/Yaha.M	7.5	--
Worm/Sobig.A	6.1	--
Worm/Lovegate.F	5.4	--
Worm Sircam.A	5.1	2.3
W32/Funlove	3.4	--
W32/Nimda	2.8	1.3
W32/Elkern	2.7	11.8
Worm/Bugbear	2.5	--

PEOPLE, ENTITIES MARKED AS INVOLVED IN TERRORISM

The Treasury Department's Office of Foreign Assets Control also publishes a list of individuals and entities that it considers Specially Designated Nationals and Blocked Persons, or SDNs, with whom the federal government forbids dealings by financial institutions, because they are suspected of engaging in terrorist-related activities. SDNs added to date in May 2003:

Gulbuddin Hekmatyar; Ansar Al-Islam; The Islamic Regiment; The Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs, and Islamic International Brigade

ENTITIES PLACED ON WATCH IN '03



Source: U.S. Department of Treasury

RECENT CIVIL PENALTIES IMPOSED BY TREASURY

These penalties were imposed by the U.S. Department of Treasury's Office of Foreign Assets and Control and made public during the two weeks that ended May 9.

Company	$settlement
Bank of the West	72
Playboy Enterprises Inc.	27
Voices in the Wilderness	20
BRI Inc./Bellwether	16
Dewey Ballantine LLP	13
United Marine Ltd.	14
Deutsche Bank AG	5
Deutsche Bank AG	4
Scientific Games Inc.	3
LKC Technologies Inc.	2

RECENT PERFORMANCE OF PUBLICLY TRADED SECURITY COMPANIES

Company	Ticker	Price 5/9	Price 4/30	2-wk ch.(%)	P/E	52-wk Hi	52-wk Lo	Shrs.Out.*	MarketCap*	Avg Volume*
Alanco Technologies Inc	ALAN	0.46	0.47	-4.5	n/a	0.74	0.23	20.1	9.6	18,409
Blue Coat Systems	BCSI	6.7	6.9	-2.9	n/a	6.99	2.05	8.88	59.4	16,181
Brink's Co.	BCO	13.27	12.75	4.1	14.58	28.41	12.36	54.3	756.8	250,818
Compudyne Corp.	CDCY	7.35	6.95	5.7	30.62	17.87	4.8	7.82	58.6	28,636
Checkpoint Systems Inc.	CKP	14.14	13.35	1.8	18.85	15.9	8.55	32.7	466.3	159,090
Diversified Security Soln.	DVS	6.75	6.9	-2.2	112.5	7.7	6.3	5.14	34.2	9,363
Entrust Inc.	ENTU	2.66	2.51	6	n/a	4.65	1.98	63.5	172.1	268,454
ICTS International NV	ICTS	5	5	0	0.62	10.299	4.75	6.51	32.2	6,954
International Electronics	IEIB	2.99	2.75	8.7	15.74	6.89	2.15	1.61	4.8	1,363
Invision Technologies Inc.	INVN	24.99	23.83	4.9	4.05	37.5	17.42	17.1	427.5	679,318
Internet Security Systems	ISSX	14.41	13.11	9.9	96.07	26.77	9.85	49.4	735.9	1,454,136
Kroll Inc.	KROL	24.25	22.3	8.7	29.57	26.96	16.35	40	986	411,681
Lojack Corp.	LOJN	4.88	4.84	0.8	27.11	5.6	3.35	14.7	710	18,454
Magal Security Systems	MAGS	6.1	5.45	1.9	26.52	12.4272	4.57	7.36	45.7	12,090
Markland Technologies	MKLD.OB	0.13	0.2	35	n/a	0.55	0.01	307.1	39.9	53,681
Napco Security Systems	NSSC	8.26	8.35	-1.1	16.52	10.2	5.58	3.43	28.3	6,818
Network Associates Inc.	NET	12.16	11.43	6.4	27.02	22.23	8.14	156.4	1,930	2,506,636
Protection One Inc.	POI	1.48	1.49	-0.7	n/a	3.32	1.25	98.1	145.2	6,318
Rainbow Technologies Inc.	RNBO	9.5	8.96	6	n/a	10.57	2.84	26.7	251.8	157,500
RSA Security	RSAS	9.75	9.54	2.2	n/a	10.22	2.23	57.5	564.4	689,363
Safenet Inc.	SFNT	25.77	23.73	6.5	n/a	32.48	10.37	9.99	278.2	262,590
SEC Associates	SAI	n/a	n/a	n/a	n/a	2	0.15	9.17	n/a	n/a
Silent Witness Enterprises	SILW	4.19	3.95	6.1	15.93	6.83	2.5	7.5	31.9	3,181
Universal Guardian Hold.	UGHO.OB	1.4	1.9	-6.3	n/a	4.8	0.2	15.2	22.8	5,727
VeriSign Inc.	VRSN	11.77	12.41	-5.2	n/a	12.5	3.92	238.6	2.885	3,611,636

** in thousands*

Compliance

WILL CALIFORNIA GET STRICTEST PRIVACY LAWS?

Banks in California may one day operate under the nation's strongest financial privacy protection initiative for consumers.

The measure being circulated by **Californians for Privacy Now**, comprising the **AARP, Consumers Union, Consumer Federation of California** and **E-Loan Inc.**, would, if passed, require financial institutions to obtain explicit consent from a consumer before selling or sharing that person's financial information with affiliates or third-party companies for any purpose other than to complete a transaction initiated by the consumer.

The measure was cleared for circulation by Attorney General **Bill Lockyer** earlier this month and now must receive 373,816 signatures of registered California voters within 150 days to qualify for the March 2004 ballot.

For more information on Californians for Privacy Now, visit www.californiaprivacy.org.

PATRIOT ACT EXPENSES

continued from page 1

Dennis Ambach, director of government relations at e-Funds, a mutual funds firm.

"The authorities say, 'We strongly recommend that you verify that information,' but regulators [appear to be adopting] a one-size-fits-all approach," Ambach said. "The large resources that Wells Fargo & Co. has are different compared to the resources available at a smaller bank."

HOW MUCH IS ENOUGH?

Then, there is the question of how much verification is actually necessary.

"There's a situation where some banks may feel that just looking at some kind of government identification on the documents is sufficient for verification when someone opens a new account. The regulation, based on the way it is worded, does not have much teeth," said **Dan Sanden**, product manger at e-Funds.

Some security officers maintain that the regulations leave open too many possibilities for error by ill-trained or under-resourced compliance staffs.

"There is the requirement that when a bank receives a document for identity verification, the date that the document was issued and its expiration date have to be recorded," he said. "Many banks record the expiration date, but it's hard to say how many will record the date the document was issued, which is in the final rule," said **Michael Kelsey**, corporate anti-money laundering officer for PNC Bank.

IS 30 MILLION ACCOUNTS TOO MUCH?

The larger the bank, the more challenging is customer verification. Global banks potentially can start 10 million to 30 million accounts each day, said **Dale Simonson**, senior manager of the **Cap Gemini** financial consulting practice of **Ernst & Young**.

Although banks have been given some latitude to determine how to practically implement customer-identification procedures, many security experts said the industry should expect to see mounting concerns around how to implement such procedures while grappling with their own customer privacy standards.

"The regulations are gray on what every financial institution should do," said e-Fund's Ambach.

GOVERNMENT DEMANDS

Already, staffing issues have come into play in another aspect of the regulation, which allows law enforcement officials investigating terrorist activities to bypass subpoena filings when requesting customer bank records.

Banks are being virtually inundated by requests by the government on suspicious consumers, said **Saskia Rietbroek**, executive director of the Miami-based **Association of Certified Anti-Money Laundering Specialists**. Even after a public comment period, when banks asked that government officials only request information when it is urgently needed, banks still say that requests for records are continuing virtually unabated.

"It's still too much," Rietbroek said. "These improvements have not made [bankers'] lives any easier."

Compliance staff would prefer to handle only those government requests for information that have a degree of urgency — not just your typical request.

"It's more reasonable to ensure that this information request process is being utilized only when it is to meet the needs and intent of Congress, and not for some type of shortcut when there is no urgency," Kelsey said.

FACTOID

45% of Fortune 1000 respondents to an industry survey employ contract security staff.

Source: *Access Control & Security Systems*

Compliance

FTC PRIVACY RULES HAS I.T. MANAGERS FLUMMOXED

The hallmark of the Federal Trade Commission's newly released security rules is flexibility — but that's exactly what's worrying some IT managers.

"Anyone managing customer data should be worried about it," said **Dennis Behrman**, an analyst at **Meridien Research Inc.** in Newton, Mass. The expectation is that the FTC will not issue guidelines requiring use of specific technologies, but it may restrict specific business practices, such as encryption of transported or stored data, he said.

The so-called Safeguards Rule, which aims to ensure adequate protection of consumer information, including electronic records — requires that companies that deal with consumer credit develop and implement appropriate safeguards to protect customer information and adequately ensure that third parties do the same.

Yet, some are expressing concern that the rule does not detail the extent to which financial institutions should go to ensure that safeguards are in place at third-party institutions with which they share customer information, or the level of compliance that would be required of third parties themselves.

"If the third parties are not adhering to the same strict set of standards as the financial institution itself, they potentially can share customer information with other third parties," said **Thomas Hinkel**, president of **Secure IT Partners Inc.**, a consultancy in Tequesta, Fla. "If there is a breach that occurs two or three levels removed from the institution, it still is a problem for the institution because they will be held responsible."

The FTC said that it would not tell each institution how to set up specific safeguards.

"Each business is its own expert on how to create and implement their own safeguard plan," said **Laura Berger**, an attorney in the division of financial practices for the FTC. "We set the program out, but we leave it to them to develop [a specific program] within the parameters contained within the rules."

The FTC "could have taken it further than they did in this rule if they wanted to," said **David Bender**, an attorney at **White & Case LLP**, New York. "This rule may have fewer specifics in it than other rules from them do. I don't know why."

The rule requires financial institutions to designate one or more employees to coordinate its information security program, to assess risks, and to implement safeguards to address those risks. The regulations do not, however, indicate a specific compliance roadmap. The Gramm-Leach-Bliley Act requires only that institutions take steps to safeguard consumers' personnal information. Any clarification of that requirement will be made by the courts, said Secure IT's Hinkel.

"A lot of institutions are waiting for the specifics of this to be defined in the courtroom," he said. "The attorneys will explain how far a financial institution will have to go to be reasonable and appropriate in complying with the regulations."

COMM-PROTECTION AT COMERICA

Comerica Inc. has tapped **Cyber-Ark Software Inc.** to secure its internet-based communications.

Detroit-based Comerica's Treasury Management Services, which provides electronic solutions to the bank's customers, is using Cyber-Ark's Inter-Business Vault to more quickly set up accounts, such as reconciliation services and automated receivables processing, as well as to streamline delivery and operations. The proprietary "Vaulting" technology of Cyber-Ark, Dedham, Mass., provides secure communications between financial services and customer clients through an automated electronic information exchange. The technology is designed to eliminate the need for programmers from banking companies to work through the problems of interacting with the specific information technology system and communications protocols of each customer.

Comerica is one of the nation's 20-largest financial institutions with $56 billion of assets.

For more information, visit www.cyber-ark.com.

BANKSECURITYNEWS
a Royal Media Group publication

Ross Priel
MANAGING EDITOR
rpriel@royalmedia.net

Carol Carangelo
SENIOR EDITOR
ccarangelo@royalmedia.net

Mike Gibb
Rob McGann
Tracy McNamara
Marianne Sullivan
CONTRIBUTING EDITORS

Jonathan S. Hornblass
PUBLISHER
hornblass@royalmedia.net

Meredith Krantz
ADVERTISING
mkrantz@royalmedia.net

Danielle Cattani
CONFERENCES
dcattani@royalmedia.net

Bank Security News is published every two weeks except in September and December, during which it is published monthly.

Subscription: $489 (24 issues).

Contact:
Royal Media Group
1359 Broadway, Suite 1512
New York, NY 10018
T: (212) 564-8972
F: (212) 564-8973

www.banksecuritynews.com

Corporate Protection

REPORT: IT BUDGETS TO RISE IN '03

A substantial number of IT leaders in the financial services sector expect to boost their technology budgets in 2003, according to a report released last month.

The Management Solutions and Services Group at **Deloitte & Touche** and **IDG Research Services Group**, which published the report, "Achieving, Measuring and Communicating IT Value," found that 47% of financial services chief information officers anticipate increasing their IT expenditures during the year. In comparison, 14% of the respondents indicated that their technology budgets will shrink in 2003.

The report surveyed 200 IT executives in the financial services (and other organizations) with revenues that range from $250 million to $5 billion.

To download the report, go to http://www.deloitte.com.

STEMMING "SILENT" ATTACKS

continued from page 1

The most famously publicized example of such misbehavior occurred at the former **Barings Banks** in London in 1995, when currency trader **Nick Leeson** used his access to the corporate server to infiltrate the system and begin trading larger amounts than he was supposed to. Although the bank had procedures in place to prevent hackers and other threats, it had no such system to detect that the trader was committing the acts until long after the damage was done.

Some silent attackers use automated phone dialing, which is also known as "war dialing," to discover an unsecured modem that can allow access to a company's operating system, or "war driving," which refers to using devices while driving past buildings to find non-encrypted wireless networks.

> "What's lacking is the proper auditing system that would be able to lessen the chance for an attack."
>
> **Michael Poor**, instructor, **SANS**

Damage, meanwhile, can take the form of a denial-of-service attack that can compromise the security of hundreds of thousands of computers across the internet and allow the installation of specific software that can sever network connectivity and impede processing and bandwidth capabilities.

Indeed, many of the nation's leading financial institutions have procedures in place to deal with an attack once it occurs, such as servers with protective tools in place to protect against and set alarms in response to unusual penetrations or transactional activity, and even security protocols that encompass servers that handle the internet, telephone, fax, and email, but most lack strategies to detect and prevent such attacks before they happen, said **Michael Poor**, an instructor for **System Administration, Auditing, Networking and Security** (**SANS**), a cooperative research and education organization.

"What's lacking is the proper auditing system that would be able to lessen the chance for an attack," he said.

A bank firewall, for example, can be infiltrated by an experienced hacker, he said.

Some banks have decided to deal with the problem with a balance of restrictions and protection. **Union Bank of California**, for example, does not allow employees to use virtual private networks, which are closed-end electronic networks, said **Bob Justus**, vice president of corporate information security and IT contingency planning for the San Francisco-based firm.

"The approach is to use encryption and password-level protection, and limit the access of employees to certain servers," he said.

Many industry experts claim that the best way to manage the threats is through the use of human, rather than technical capital. One company in the financial services sector did not install IT security staff in its operations until two years ago, said Poor. That is just one example of how the way in which personnel who manage information security are staffed can threaten bank security, he said.

The ideal solution is for banks to designate a team that is responsible for overseeing every single connection made from private networks to servers, and set up specific procedures so that everyone must go through that team to gain access, Barney said.

Ted DeZabala, a partner in the Enterprise Risk Service Group of **Deloitte & Touche** and director of that company's Security Services practice, suggested platform standardization, which can alleviate security vulnerabilities. "If you have 30 different operating systems, you can definitely reduce that number to 15. That way, you lower your exposure by half," he said.

People Scan

FAIRBANKS CAPITAL APPOINTS COMPLIANCE CHIEF

Fairbanks Capital Corp., one of the nation's leading subprime residential mortgage servicers, has appointed **Valorie Kacherian** to the position of chief compliance officer.

Kacherian, who most recently served as vice president and chief compliance officer for the **HomeEq Servicing Corp.** division of **Wachovia Corp.**, is overseeing compliance operations at the Salt Lake City-based Fairbanks, which services more than 550,000 residential mortgage loans annually.

A 30-year veteran of the financial services industry, Kacherian has held executive positions at **Statewide Mortgage Co./Norwest Home Improvement** and **NationsBank/NCNB** (**now Bank of America Inc.**)

TOUMA TAKES I.T. POST AT PROVIDENT

Provident Bank has hired **Raymond Touma** as vice president of information technology.

In his new position, Touma is overseeing the Montebello, N.Y.-based bank's system and network security. He also is responsible for managing information systems as well as technology planning and implementation. In addition, Touma is in charge of the development of the financial services provider's overall technology program.

Prior to joining Provident, Touma held the post of vice president of information technology at **Banco Popular North America**. He also was manager of network services for **Universal American Financial Corp**.

Provident, which has more than $1 billion of assets, operates the only trust department headquartered in New York State's Rockland County.

NEW CLO FOR BANK ONE

Bank One Corp. has found a chief legal officer.

Last month, Bank One hired **Joan Guggenheimer**, a former general counsel of the global corporate and investment bank for **Citigroup**, to head up its legal affairs

In addition to serving as CLO and head of the law, compliance and government relations department, Guggenheimer also is on the planning group comprised of Bank One's executive management.

She reports to chairman and chief executive **Jamie Dimon**.

Bank One has assets of more than $275 billion, making the Chicago-based firm the sixth-largest bank holding company in the United States.

BARCLAYS TABS COMPLIANCE EXEC

Barclays Capital has hired a new executive to head its compliance operations.

Earlier this month, the New York-based investment banking subsidiary of **Barclays PLC** appointed **Erin Mansfield** to the position of director and head of compliance for the Americas.

Mansfield joins Barclays Capital from **Goldman, Sachs & Co.**, where she most recently served as senior compliance officer of credit markets and credit derivatives. Among other responsibilities she managed compliance issues that were related to the nation's credit markets and credit derivatives globally. At Goldman, Sachs Mansfield also held the post of vice president of fixed income, currencies and commodities division.

Mansfield reports to Barclays chief administrative officer for the Americas **Gerard LaRocca** and to **Stephen Morse**, global compliance chief.

BANKERS SYSTEMS BRINGS IN CTO

Randy Mueller has joined **Bankers Systems Inc.** as the company's senior vice president and chief technology officer.

Mueller, who previously was a senior executive at **Marquette Financial Cos.**, is overseeing numerous functions for the St. Cloud, Minn.-based supplier of compliance resource solutions to the financial services sector. His responsibilities include leading the vendor's internal information technology operations. In addition, he also is in charge of Bankers Systems's development of software products and is managing the company's technical services and support for the bank, credit union and mortgage markets.

HARTFORD TAPS PROPERTY-AND-CASUALTY OPS VP

Hartford Financial Services Group Inc. has created the position of senior vice president of corporate asset protection for its property and casualty operations.

The company has appointed **Robert Paiano**, who formerly was a senior vice president and director of the investment strategy group for **Hartford Investment Management Co.**, to serve in the position.

Paiano's responsibilities include heading the company's security review. In addition, he is in charge of Hartford Financial Services' corporate risk and catastrophe management, insurance and reinsurance purchasing and growth strategies.

Paiano also oversees Hartford Financial Services' ceded reinsurance operations in Bermuda.

Innovations

PRACTICAL SECURITY IDEAS AND SOLUTIONS

AURUM WINS IT OUTSOURCING CONTRACT

Aurum Technology won the contract to manage **North American Savings Bank**'s information technology.

Financial terms of the contract were not disclosed.

Aurum will start handling North American's IT, including its security management and customer signature verification system, in November.

Aurum is based in Plano, Texas; North American in Grandview, Mo. North American has about $1 billion of assets and services the greater Kansas City, Mo., area.

Aurum's clients include Cardinal Bank, Fairfield, Va.; United Heritage Credit Union, Austin, Texas; IC Federal Credit Union, Fitchburg, Ma.; Southern Commercial Bank, St. Louis; and Capital Bank, Rockville, Md.

For more information, visit www.aurumtechnology.com.

PATRIOT ACT FORCING TOUGH CHOICES ON OUTSOURCING

The heightened degree of compliance required by the Patriot Act and new consumer identification regulation is forcing banks to make a choice: Whether to use vendors or in-house staff to manage the task of complying with the new regulations.

"Banks have to go through their own risk assessment and then make a decision based on what makes sense to them," said one bank executive. "The factors [to be weighed] include the size of the institution, the nature of the customer base, and so on."

Implementation plans also hinge on the status of compliance regulation at the particular bank. Some banks have been wary of investment in potentially costly tools until the final scope of a rule has become clear, said **Saskia Rietbroek**, executive director of the Miami-based **Association of Certified Anti-Money Laundering Specialists** (**ACAMS**).

The scale of the financial institution and the scope of its operations will contribute to banks' investment decisions.

"**Bank of America Corp.** and **Citigroup Inc.** cannot possibly verify all of the information manually that they receive," Rietbroek said. "That is where third-party software can come in to detect that automatically. Smaller financial institutions, on the other hand, may want to do it manually."

A number of the nation's largest financial firms, including **Citigroup Inc.**, **J.P. Morgan Chase & Co.**, **Wells Fargo & Co.**, **KeyCorp**, **Bank One Corp.**, **Union Bank of California**, **Fleet Boston Financial Corp.**, and **National City Corp.**, utilize internal resources to comply with the Patriot Act.

High compliance costs and sizable penalties for non-compliance have helped to enhance the appeal of a third-party tool alternative, however.

Anti-money-laundering compliance costs in the financial services sector are expected to reach $11 billion during the next two years. While no one can pin down the exact costs that banks and financial institutions will have to pay for tools that track suspicious activities, the number can range from the thousands to several millions of dollars.

For example, software that helps banks determine who their customers are, tracks their funds and normal transaction activity under the "Know Your Customer" provisions, can range from $1,000 for a community bank to $150 million to $650 million for larger institutions.

The cost for non-compliance can be hefty. **Broadway National Bank** in New York failed to develop a federally required anti-money laundering program, and that led to the company's $4 million fine last year.

Beyond scale and scope issues, most banks also wrestle with the larger issue of reputational risk. If banks do not adequately comply with the Patriot Act, will their reputations among consumers suffer?

"There is an increased reputational risk that every financial institution faces in today's world," said **Dirk Mohrmann**, president of **World Compliance**. "If you look at financial institutions that have been under investigation for managing or harboring funds of former dictators of certain countries, that reputational risk has moved compliance from a pure 'how do I comply with the law' approach into a risk-management tool."

World Compliance's basic compliance package offers a scalable solution via an amalgamated list with both terrorists and criminals that appear on the Treasury Department's Office of Foreign Assets and Control list as well as those that appear on approximately 20 other similar lists published by authorities worldwide.

While suppliers can provide an effective solution, the decision remains difficult for banks. "You are still responsible for compliance," said the bank executive. "You have to worry about the vendor, if they're up to standards. You can't contract away responsibility."

Tech Bytes

PRIMARY PAYMENTS DEBUTS WEB CUSTOMER ID TOOL

Primary Payments Systems Inc. has brought its customer identity verification tool to the internet.

The Scottsdale, Ariz.-based division of **Concord EFS Inc.**'s Identity Chek helps companies protect against fraud by screening checking and savings accounts, loans, credit card applications and changes of address against databases of criminal or suspicious activity or if the information or product request violates any anti-money laundering protocols. Identity Chek is being sold to small- to mid-sized financial institutions that must comply with new customer ID requirements in the Patriot Act. Many of the 30-largest financial institutions in the nation use Identity Chek, the company said.

"Frankly, the smaller institutions are where fraud has been moving in recent years," said a company spokeswoman. "As the U.S. population has become more transient and customers have become less well known to banks compared to previous years, criminals have moved to target smaller banks."

Primary Payments developed Identity Chek to perform as many as 60 different tests in order to detect inconsistent, invalid and unusual elements in each inquiry and to provide notification of these elements rapidly to its customer clients. Users of the online system pay a fee per inquiry.

For more information, visit www.primarypayments.com

THRUPOINT JOINS NETFORENSICS TO BUILD SECURITY SOLUTION

NetForensics Inc. has partnered with **ThruPoint Inc.** to develop an information security solution that will combine netForensics's expertise in network security with ThruPoint's consulting.

Edison, N.J.-based **netForensics**, a vendor of security technology, plans to work with ThruPoint to provide business development and high-level consulting to clients worldwide, including financial services providers. In addition, the companies expect to develop joint training programs that incorporate the software that netForensics develops to provide security solutions with the IT consultancy capabilities of ThruPoint. ThruPoint is based in New York.

For more information, visit www.netforensics.com or www.thrupoint.net.

VASCO LAUNCHES NEW ID TOKENS FOR AUTHENTICATION

VASCO Data Security International Inc. has introduced a pair of authentication devices for network access for use by financial institutions, among others.

Digipass 260 and Digipass 560, are part of the Oakbrook Terrace, Ill.-based company's collection of Digipass Identity Authentication hardware. The Digipass 260 is provides remote access, authentication and e-signatures via a lightweight, password-protected authentication device. The Digipass 560 is an authentication code generator.

The company's Digipass line, which is used by **Wachovia Corp.** and approximately 200 other financial institutions, affords users an alternative to fixed or static passwords, Vasco's chairman and chief executive, **Ken Hunt**, said in an announcement. The technology enables users to generate a different, one-time password with every use.

For more information, visit www.vasco.com.

CALENDAR

June 2-4
The Gartner IT Security Summit 2003 will take place at the Washington Hilton & Towers, 1919 Connecticut Ave. N.W., Washington, D.C., 800-778-1997 or *www.gartner.com/us/itsecurity*

June 11-16
The SANS System Administration Audit Network and Security Institute's Computer Security Boot Camp 2003 will be presented at the Doubletree Hotel Monterey in California. 1-866-570-9927 or *www.sans.org*

July 13-17
The 17th Annual Vanguard Enterprise Security Expo & Remote Access Control Facility Users Training 2003 will be held at the J.W. Marriott Grande Lakes Resort, Orlando, Fla. 1-888-547-3976 or *www.go2vanguard.com*

July 23-26
The National Association of Federal Credit Unions will hold its 36th annual conference and exhibition at the John Hynes Veterans Memorial Convention Center in Boston. 1-800-336-4644 or *www.nafcu.org*

checking accounts

credit cards

401Ks

loss mitigation

auto loans

interest rates

mortgages

IS MERELY HOW WE SAY *GOOD MORNING.*

:: *We are Momentic. We live consumer finance.*

Obsessively focused, Momentic provides custom research, consulting, and advisory services on all facets of finance. A team of talented consultant/researchers develop sound strategies and hardened assessments of market dynamics for financial services providers and investors. We concentrate on developing insights into the revenue, cost, and credit quality of the industry and/or particular companies with our on-the-ground, exclusive competitive intelligence.

Find out how we can help your business grow by calling 713-270-9956 or emailing ideas@momentic.com.

momentic
We Know