

BANK SECURITY NEWS

A ROYAL MEDIA GROUP PUBLICATION • 261 FIFTH AVENUE, SUITE 412 • NEW YORK, NY 10016 • WWW.BANKNET360.COM

INSIGHTS ON CORPORATE AND INFORMATION SECURITY • DECEMBER 2005 VOL. 3, NO. 10

NEWS INSIDE

TRENDS

Are cash and checks on the verge of extinction? Electronic payments catch up **page 4**

Internet banking gets a boost while consumers shun online shopping **page 4**

RESEARCH

What a data breach may end up costing you **page 5**

ON BOARD

Corillian offers a new kind of identity authentication to help banks deal with the upcoming two-factor rule **page 6**

RULES & REGS

Credit card industry beware: a new PCI compliance deadline is on the horizon **page 7**

SCORECARD

A day-by-day analysis of attacks on banks **page 9**

DEPARTMENTS

Event Calendar **page 8**

Breach Tracker **page 10**

Tech Tracker **page 10**

Equities Monitor **page 11**



2005 © Royal Media Group
All rights reserved

MORTGAGE BANKERS PREP FOR BREACHES

Mortgage banking is usually not the first segment of the financial services industry that springs to mind when discussing data breaches, but a new set of recommendations that will stem from a recently released white paper by the **Mortgage Bankers Association** intends to raise awareness of the issue before major troubles appear.

"Identity thieves and hackers will try to penetrate an area as much as possible and when they've exhausted that they move on to another," said **Yuriy Dzambasow**, principal consultant with **A&N Associates**, and a co-author of the white paper. "The mortgage industry does a lot of stuff online. We might be the next target."

The **Mortgage Industry Standards and Maintenance Organization** [MISMO], an MBA subsidiary, and its **Information Security Working Group** [ISWG] are developing best practices surrounding protecting personal information for the mortgage industry. Those practices are expected to include recommendations for collecting, processing, transferring, storing, and disposing of personal information.

The recommendations are to be released by yearend, and will be available at www.mismo.org.

Continued on page 3

DELAY POSTPONES BSA DIRECT UNTIL JANUARY

William Fox, director of the **Financial Crimes Enforcement Network**, was being facetious when he put his job on the line in April, saying he should be fired if a new project, called **BSA Direct**, was not up and running by October.



William Fox
FinCEN

Facetious or not, the project, an online database of suspicious activity and currency transaction report filings, did not meet the October deadline, and is not expected to be operational until next month. The agency, part of the **Treasury Department**, recently announced the delay without providing any further details.

BSA Direct will be capable of searching more than 15 million Bank Security Act-related reports including SARs, CTRs, and other filings from more than 25,000 financial institutions.

"While it will be a few months later than we originally hoped, the delay is not entirely unexpected for the development of a new information technology system," said **Sheri James**, a FinCEN spokeswoman. "We recognized from the outset that our schedule was quite aggressive, and have worked hard to meet that schedule."

Continued on page 3

WEB SEMINAR:

EFFECTIVE TWO-FACTOR AUTHENTICATION STRATEGIES

SPONSORED BY:



MEDIA SPONSOR:

BANKSECURITYNEWS

DATE:

Thursday March 9, 2006

TIME:

1PM EST - 2:15PM EST
(Please check your time zone
for the correct local time)

FEATURED SPEAKERS:

Jim Cowing
Managing Director
Digital Resources Group

Bruce Cundiff
Analyst
Javelin Research

Why 2? Because by the end of 2006, the federal government mandates that all banks offering online banking must include two-factor authentication for customers to identify themselves when accessing accounts.

The demands from the Federal Financial Institutions Examinations Council are steep:

- You must have a two-factor authentication process in place
- You must make sure your processes are updated, if you have one already
- You must stay in compliance

That's why you should attend our "Two-Factor Authentication: A Product Analysis" web seminar. We'll tell you which products are out there to make the transition to two-factor authentication as smooth as possible.

We have brought on board two — there's that number again — expert speakers to help you distinguish between all of the available products with a frank assessment of what works best and an eye on what the FFIEC really wants. Register today for this timely web seminar.

REGISTRATION INFORMATION

Cost: \$199 for subscribers to *Bank Security News*
\$239 for Non-subscribers
Cost is per site and allows access to one phone
line for unlimited # of listeners

TO REGISTER

Call: 800.320.4418 Option 4
Fax: 309.414.6476
info@royalmedia.com
www.royalmedia.com

BANKSECURITYNEWS



MBA TO ISSUE SECURITY GUIDELINES

Continued from page 1

"MISMO will work at drilling down and applying these concepts to the middle manager," said R.J. Schlecht, the MBA's director of industry technology. "We'll address threats and vulnerabilities and then recommend generic industry practices that organizations can use to build their policies."

The new MISMO/ISWG recommendations will comply with pending federal legislation, including the **Financial Data Protection Act of 2005**, and other state laws. It is the MBA's goal to develop a consistent method for preventing data breaches industrywide, Dzambasow said.

Meanwhile, the MBA last month endorsed the Financial Data Protection Act of 2005, while also asking the **House Financial Services Committee's** Subcommittee on Financial Institutions and Consumer Credit for some amendments. Those included: developing "more concise security triggers that will not cause lenders to be unnecessarily overburdened in providing notifications," and further specifying what qualifies as "sensitive financial identity information." —MOLLY BROWN

FINCEN DIRECTIVE DELAYED

Continued from page 1

FinCEN aimed for a complete delivery of the IT system within 16 months, James said.

In April, Fox told *Bank Security News* that if BSA Direct was not in place by October, that he "should be fired."

"Mr. Fox continues to be eager to launch BSA Direct and while he had hoped it would be launched in October, he is very committed to the launch of this major system and wants to ensure that is rolled out when it is fully tested and operational," said a FinCEN spokeswoman in an email.

"FinCEN is closely working with law enforcement and regulatory officials to "keep them apprised of developments related to the system," and has an outreach plan to roll out BSA Direct when it is ready, James said.

BSA Direct — the "secure, web-based, modern data query, and analytic tool" — was developed to help in money laundering, financial crime, and terrorist financing investigations, Fox said in an April with editors of *Bank Security News*.

Continued on page 4

MORTGAGE INDUSTRY WHITE PAPER ADDRESSES FRAUD

The **Mortgage Bankers Association** in October released a white paper, titled "Protecting Personal Information: The Good, the Bad, the Ugly."

The **Federal Bureau of Investigation** reports that instances of mortgage-related identity theft are increasing. There were 642 pending home loan fraud cases in May 2005, up from 534 at the same time a year earlier, and the number of mortgage-related Suspicious Activity Reports filed with the **Financial Crimes Enforcement Network** jumped to 17,127 in 2004, from 6,936 in 2003. Mortgage fraud causes \$429 million in damages, according to a FBI report.

"Identity theft has been on a dramatic increase in the mortgage lending area in the past several years," said **John Simon**, vice president of technology initiatives with Atlanta-based **LandAmerica Credit Services Inc.**, a supplier of credit reports. "Identity fraud is not as large as other types of mortgage fraud, but it's growing."

The FBI mortgage fraud report did not specify how many cases involved ID theft, but "to say a vast majority involve identity theft is a fair statement," according to a FBI spokesman.

Targeted to executive-level managers, the MBA paper focuses on why mortgage bankers should tighten online security and educate consumers about identity theft and fraud. It is a message most mortgage bankers are happy to hear.

"These are the things mortgage bankers really need to look at internally," said **Randy Zuendel**, information security officer for Highland Hills, Ohio-based **DeepGreen Financial**, an online home equity lender. —M.B.

STAFF

BANK SECURITY NEWS

EXECUTIVE EDITOR
& PUBLISHER
JJ Hornblass
hornblass@royalmedia.com

ASSOCIATE EDITOR
Molly Brown
mbrown@royalmedia.com

SENIOR EDITORS
Marcie Belles
mdblles@royalmedia.com
Mike Gibb
mgibb@royalmedia.com

CONTRIBUTING EDITORS
Stephen Bernard
Patricia Churpakovich
Vincent Ryan
Mike Sherrill

STAFF REPORTER
Aaron Johnson

PRODUCTION EDITOR
Ethan Byun
ebyun@royalmedia.com

EVENTS
Danielle Cattani
Molly Devine
Heather Sina

MARKETING MANAGER
Stephen Sullivan

CUSTOMER SPECIALIST
Naima Hernandez
nhernandez@royalmedia.com

ADVERTISING SALES
Meredith Krantz
mkrantz@royalmedia.com

DIRECTOR, WEB SERVICES
Edward Song

Bank Security News is published monthly. Annual subscription: \$419 (12 issues).

Tax ID #13-3852425. For more information, contact
Royal Media Group
261 Fifth Avenue, Suite 412
New York, NY 10016
T: (212) 564-8972
F: (212) 564-8973
E: connect@royalmedia.com
www.royalmedia.com

2005 © Royal Media Group

WARNING!

It is illegal to photocopy or reproduce any part of *Bank Security News* without the written consent of Royal Media Group. Call (212) 564-8972 to obtain duplication rights.

IN BRIEF

TRANSUNION LATEST TO EXPERIENCE DATA BREACH

TransUnion LLC, owner of one of the largest consumer credit databases, announced that a desktop computer was stolen in early October from one of its California offices, according to a company statement.

The computer reportedly held personal information of about 3,600 consumers, according to the statement.

In response, TransUnion notified local law enforcement and has initiated an internal investigation. The company also sent notifications, with a toll-free number for its fraud victim response team, to customers affected by the breach.

Customers are also being offered free copies of their credit reports from TransUnion, as well as from the other two major credit bureaus. Customers can use these free services for a year, and are able to place a fraud alert on their file.

TransUnion is also internally monitoring potentially-affected consumers' credit reports, and does not "believe there is any indication of any fraudulent activity" at this time, according to a statement. —M.B.

Continued from page 3

Last spring, FinCEN also estimated that at least 40% of all BSA filings would be submitted electronically by the end of 2005, which allows financial institutions to access BSA reports faster. The agency reports that it is on track to reach this goal, James said.

BSA Direct is in response to the USA Patriot Act Section 361 mandate which states that FinCEN must establish and "maintain a government-wide data access service, with access to ... information collected by the Department of the Treasury, including report information," according to a FinCEN statement. —M.B.

TRENDS

ELECTRONIC PAYMENTS GAINING ON CASH, CHECKS

Online electronic payments now means more than just buying things on eBay or Amazon.com.

More consumers are embracing online bill payment, at the expense of cash and check transactions, according to a study by the American Bankers Association released in late October.

More than half of the consumers surveyed revealed that they pay at least one bill a month online, and 39% are going to the web for multiple bill payments, according to the study. Checks now account for fewer than half of the respondents' monthly bill payments, down from 72% in 2001.

Going forward, consumers estimated that they will use 23% fewer checks to pay bills during the next two years.

"When you talk about paying your bills, it's not something that has a particular sexiness to it," said Tom Carey, vice president of MasterCard's Remote Payment and Presentment Service. "Making an easier way to do this undesirable chore is going to attract more people."

Now that the initial fears associated with online bill payment appear to be subsiding, consumers are finding that using the web to pay bills can actually act as a safeguard in the battle against identity theft and fraud.

"Customers find problems sooner when they check accounts online," said Matt Lewis, vice president of the electronic commerce division at CheckFree, an Atlanta-based payment services company which counts U.S. Bancorp and Wachovia Corp. among its clients. "Users can react to changes in accounts in real time versus waiting for a paper statement."

The growth in online bill payment may lead to more consumers banking online, too. Online banking will continue to grow as more institutions implement two-factor authentication methods, said Jane Yao, the ABA's managing director of survey research.

"Our customers, banks, service providers, and processors do reach out to customers," Carey said. "It's a sensitive message for banks — you have an interest to want consumers to feel confident about their bank." —M.B.

ONLINE BANKING GROWS, DESPITE FEARS ABOUT WEB USE

Consumers not only trust banks with their life savings, but also their identities as well, according to the results of a new study.

While concerned about offering personal data online, a preponderance of consumers trust the safety of online banking, according to the study, conducted by Consumer Reports WebWatch, a joint effort between Consumer Reports magazine and other consumer organizations.

"It's good news for online banking that American consumers have a relatively high degree of trust in the sites they use."

—Beau Brendler, Director, Consumer Reports WebWatch

More than two thirds of consumers trust their financial institutions' web sites, even as 30% of internet users reported that they have reduced their overall online use due to fears about fraud.

"It's good news for online banking that American consumers have a relatively high degree of trust in the sites they use," said Beau Brendler, director of Consumer

Continued on page 5

Continued from page 4

Reports WebWatch. "The nature of choice among those types of companies is a trust one, and I think the trust relationship is already built in."

But a trust-factor gap still exists between those who do bank online and those who have yet to take the plunge. Nearly 93% of those who use online banking said they trust it, while only 48% who do not bank online think it is safe. This illustrates that those who bank online like it, while institutions must continue to work to build trust with non-users, Brendler said.

At many institutions, more consumers are flocking to online banking. The volume of customers using online banking at Akron, Ohio-based **FirstMerit Bank**, for example, has increased 15% this year, to 200,000 users, said **Jim Giarrano**, the bank's vice president of client service development. The bank has updated its site, adding numerous functions, and its customers have responded, he said.

Banks are showing their sensitive sides, too. To alleviate consumer fears, more institutions are

FAVORED ONLINE BANKING SERVICES

Banks' web sites received positive feedback from U.S. internet users in a recent study by **Consumer Reports WebWatch**, with 68% reporting that they trust the information provided and think the sites are safe to use.

According to Consumer Reports, here are internet users' preferred online financial activities:

- 45% use online banking
- 24% use credit check sites
- 23% use automatic bill payment
- 12% use stock and mutual fund sites
- 7% use mortgage and loan sites

The report is good news for the internet banking industry as users curb other habits like shopping online. Overall, 30% of consumers said they have reduced their internet use, and 29% reported that they have cut back on making online purchases, according to the results. —M.B.

rolling out enhanced security measures on their web sites. **Bank of America Corp.**, for example, is expanding its online authentication program, SiteKey. Already available in 20 states, SiteKey requires users to select an image and write a brief phrase. This information is shared with Bank of America, forming multiple levels of online authentication, according to a company statement. —M.B.

RESEARCH

NEW STUDY QUANTIFIES THE COST OF DATA BREACHES

While legislation has required companies to be more vocal about data breaches, the companies, including financial institutions, have been silent about how much it costs to deal with a breach. New research reveals, however, that the average incident costs \$14 million, including direct expenses, as well as the loss of current and potential customers.

But security advisers felt the study lowballed the costs.

The study is "very helpful as far as putting a stake in the ground as far as costs," said **Jim Reavis**, president of Ferndale, Wash.-based **Reavis Consulting Group**, a security strategies company, and a board member of the **Information Systems Security Association**. "It's very sobering — the cost-per-loss record — but I think there are a lot more breaches out there than are being reported."

Between February and October, there were more than 80 data-breach announcements resulting in more than 50 million customer notifications, according to the survey, conducted by Elk Rapids, Mich.-based **Ponemon Group** and sponsored by **PGP Corp.**, a Palo Alto, Calif.-based security-solutions provider. Ponemon Group analyzed data from 14 U.S. companies' data breaches, including two financial institutions, in determining the costs of a breach.

The study measured direct expenses incurred, including investigations, notification letters, and legal services. It also quantified indirect expenses such as the hit to employee productivity, and the cost of future business, including the loss of new customers and reputation damage.

Continued on page 6

IN BRIEF

BANK OF NEW YORK RESOLVES AML LAWSUIT

Bank of New York reached a \$38 million settlement on Nov. 8 with U.S. attorneys' offices in Manhattan and Brooklyn, N.Y., the largest fine for money laundering violations ever assessed against an American bank, thus ending a six-year investigation.

The Bank of New York will pay a \$26 million fine to the government and \$12 million in victim compensation. The bank also agreed to adopt "sweeping internal reforms to ensure compliance with its anti-fraud and money-laundering obligations and be monitored by an independent examiner," according to a statement released by the prosecutors' offices.

As part of the agreement, the bank will not be prosecuted for unlawful practices if it remains compliant with the government's terms for three years, according to the prosecutors' statement. —M.B.

JOIN THE DIALOGUE

Do you have questions, comments, even criticisms about stories in *Bank Security News*? Or is there information you'd like to see us publish? We want to hear from you.

Give us a shout if you have news you want published, a recent hire you want to tout, or you have put in place a new business strategy.

Associate Editor **Molly Brown** can be reached at 212-564-8972 x103 or mbrown@royalmedia.com.

Continued from page 5

The findings reveal that the average data breach costs a company about 20% of its existing customers, while another 40% consider terminating business ties.

"It's difficult to put an average cost on an instance of data breach. Each event is unique and presents its own challenges."

—Aaron Albright, Spokesman, American Bankers Association

"Let's not forget that many, if not most of these costs, could be avoided had these companies adopted effective security strategies years ago," said **Beth Givens**, director of **Privacy Rights Clearinghouse**, a San Diego-based consumer advocacy group that tracks data breaches. "Many of these costs are really a form of catch-up."

The study is one of the first efforts to apply dollar losses to breaches and quantify the effects of fraud on a company's well-being, said **Andrew Krcik**, PGP's vice president of marketing.

Bankers were reluctant to offer their views on the costs associated with a data breach.

"It's difficult to put an average cost on an instance of data breach," said **Aaron Albright**, a spokesman for the **American Bankers Association**. "Each event is unique and presents its own challenges. We do agree that data breaches can hit institutions with serious financial and reputation costs."—M.B.

ON BOARD

CREDIT UNION PICKS CORILLIAN AUTHENTICATION

The **University of Wisconsin Credit Union** will be the first financial institution to use Hillsboro, Ore.-based security provider **Corillian Corp.**'s Intelligent Authentication security solution designed to prevent fraud in online banking.

The Madison-Wis.-based credit union, which has \$800 million in assets and more than 100,000 members, announced that it will

implement the increased security-authentication application by early this month. The move will bring it closer to meeting the **Federal Financial Institutions Examination Council's** end-of-2006 deadline for implementing two-factor authentication systems, said **Eric Bangerter**, the institution's director of internet services.

"We didn't want something that was overly intrusive," Bangerter said. "Corillian did it very quickly. It's taken about nine months for them to develop the product, and we're in the final stages of putting it in place."

Although what the credit union is implementing is not a full two-factor authentication solution, it allows for additional security measures to be added when the credit union is ready to upgrade. The credit union plans to test the system throughout 2006 and add functions as needed, Bangerter said.

Corillian's Intelligent Authentication product monitors a customer's email, connection, and location, and asks security-based questions to determine identity.

The product "offers up to four layers of protection," said **Jim Maloney**, Corillian's chief security executive. "And the system upgrades itself automatically in case of fraudulent behavior."—M.B.

M&T BANK ENHANCES SECURITY

Buffalo, N.Y.-based **M&T Bank Corp.** has signed on to use the Web Application Gateway offered by Santa Clara, Calif.-based security provider **Teros**, to guard the bank's online mortgage center from malicious internet attacks.

One of the nation's largest bank holding companies, with \$52 billion in assets and 650 branches throughout the East Coast, M&T Bank is the newest financial institution to join Teros's client. Other clients include Birmingham, Ala.-based **Regions Bank**, and Carmel, Ind.-based **Baker Hill**, an internet-services provider for loan processors that serves about 120 commercial banks nationwide, said Teros Chief Executive **Bob Walters**.

"Most banks don't have IT staffs to figure out complex problems," Walters said. "We are secure, we do what we say, and it works."

M&T declined to comment. —M.B.

RULES & REGS

NEW PCI-COMPLIANCE DEADLINE ON HORIZON

In financial services, the 12 steps are taking on a whole new meaning.

The large players in the payment card industry [PCI] — Visa, MasterCard, American Express, and Discover — have outlined 12 steps that banks, merchants, and service providers need to accomplish to remain compliant with their data-protection standards.

But months ago Visa set a deadline for companies to be in compliance, and many banks, merchants, and service providers are still trying to get up to code, according to a SysAdmin, Audit, Network, Security [SANS] Institute presentation last month.

So Visa has set another deadline — Dec. 31

— for industry-wide compliance, which all PCI-endorsing credit card companies will adhere to, according to a Visa spokesman.

Visa would not disclose how many banks, merchants, and companies are PCI compliant, but a high number of them have “not only started the process, but are fairly well through it,” said Joe Majka, vice president for Visa USA Fraud Control.

The new PCI standard evolved from the December 2004 alignment of Visa’s Cardholder Information Security Program and MasterCard’s Site Data Protection Program. Its steps include installing firewalls, protecting stored data, and encrypting sensitive information. Failure to meet any of the 12 steps results in non-compliance, Majka said.

“Many tell us they do secure data but it may not be quite up to the standards we have in

Continued on page 8

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Here are the 12 steps needed to comply with the new PCI standard.

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored data
- Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

Source: Visa U.S.A. Inc.

SHARE THE WEALTH

As a reader, you know how valuable *Bank Security News* is. And we want to help you share its wealth of knowledge and insights with your colleagues.

Now you can buy a subscription for everyone in your company at one low price, no matter how large your department or institution. Known as a site license, the yearlong subscription costs \$3,500 and is easy to manage. We give you a special email address and you simply direct your colleagues to use it to request the publication at any time during the year. We take care of the rest.

Of course, a site license protects you from possible copyright infringement. As you may know, readers are not permitted to copy and distribute *Bank Security News* without the written consent of its publisher, Royal Media Group.

To find out more about the site-license program, please contact Meredith Krantz at 212-564-8972 x101 or mkrantz@royalmedia.com.

Continued from page 8

place," Majka said. "We set up a pretty high standard, but feel the industry standard should be met."

Organizations trying to comply are still confused, according to Visa PCI compliance assessors.

"Just documenting the procedures and processes, there are very specific requirements around that," said **Alan Ferguson**, vice president and co-founder of Boulder, Colo.-based **Coalfire Systems Inc.**, a Visa-approved PCI compliance assessor. "I would say that is the one common gap."

The standard PCI audit includes interviews, data collection, technical testing, and reports on compliance and security activities. Based on the size of an organization, it takes from three to six weeks to complete, Ferguson said.

And organizations have been slow to dedicate resources to PCI compliance.

"I don't know anyone who puts PCI compliance at the top of their list," Ferguson said. "Security is top of mind. Compliance isn't."

Denver-based **IP Commerce Inc.**, a software-services platform supplier for payment-services companies, has

achieved PCI compliance. Although IP does not process card information directly, it has to comply with PCI's best practices standard, said **David Johnson**, the company's vice president of technology.

Johnson agreed that the biggest obstacle to PCI compliance is developing and maintaining documentation on the processes.

"It's a great idea, but most people don't do it," Johnson said. "It's costly and incredibly painful for the industry right now."

PCI, especially the auditing process, could be improved by increasing efficiency through better communication and education, Johnson said.

The PCI standard continues to be a work-in-progress, Majka said.

"We're in the process of reviewing the current standards and making some minor changes that will be published at the end of the year," Majka said.

"But there will be no major changes in any of the 12 requirements."

Assessors recommend that any organization that handles credit card data make PCI compliance a priority to avoid fines later.

"The best advice is to gain senior

management focus around this," Ferguson said. "Getting support on the technical staff's side allows them to go ahead and implement an adequate standard." —M.B.

NEW PRODUCTS

ROYAL MEDIA UNVEILS NEW BANK INFORMATION SITE

Royal Media Group introduced **BankNet 360** this month, the 360-degree resource of everything banking, updated in real-time.

With proprietary technology and a sophisticated team of researchers, **BankNet 360** uncovers market intelligence in multiple disciplines in banking, including information security.

The site offers more than 200 email alerts on every conceivable topic and company in banking, and access to the information is available via RSS, the new technology for getting news online.

BankNet 360 is easily customized so visitors see only the news on the topics that matter to them. The site is also free.

You can join **BankNet 360** by visiting www.BankNet360.com

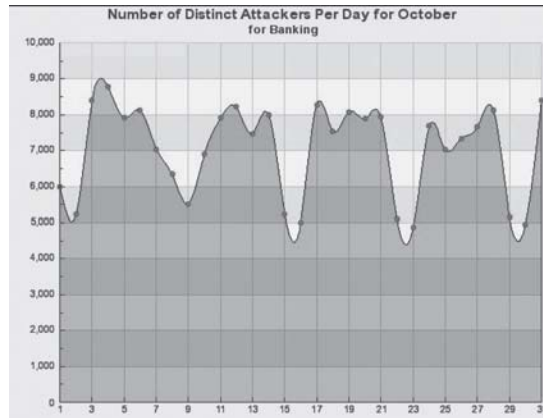
INDUSTRY CALENDAR

Date	Event	Producer	Location	Web Site
Dec. 5-8	Data Center Conference	Gartner	Las Vegas	www.gartner.com
Dec. 6-7	Finsec	MIS Training Institute	New York	www.misti.com/finsec
Dec. 6-8	Infosecurity Conference & Exhibition	Infosecurity	New York	www.infosecurityevent.com
Dec. 13-14	IP Communications for FS Firms	Info Management Network	New York	www.imn.org
Jan. 13-18	Women in IT Security	SANS	San Francisco	www.sans.org
Feb. 23	Teaming Up Against Identity Theft: A Summit on Solutions	California Department of Consumer Affairs	Los Angeles	www.idtheftsummit.ca.gov
Mar. 9	Two-Factor Authentication	Bank Security News	Online	www.banknet360.com

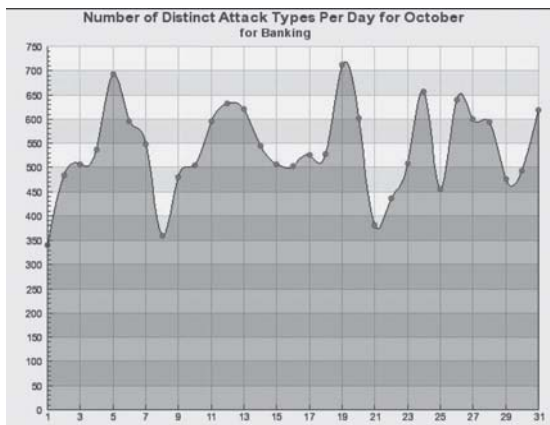
To have your event listed in the calendar, contact Molly Brown at (212) 564-8972 x103 or mbrown@royalmedia.com.

DAILY NUMBER OF DISTINCT ATTACKERS

The number of IP addresses attacking SecureWorks' 600 banking clients during October. The figure crested at 9,000 attackers on Oct. 4.



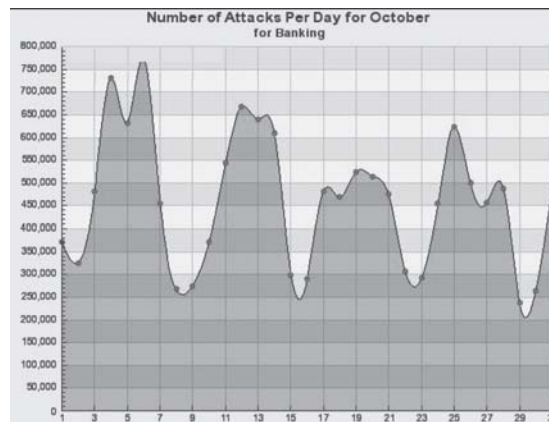
DAILY NUMBER OF ATTACKS



The number of different types of attacks — including viruses, spyware, and phishing scams — that were attempted against SecureWorks' 600 banking clients. The busiest day was Oct. 19, with more than 700 different types of attacks.

DAILY NUMBER OF DISTINCT ATTACK TYPES

The number of alerts that SecureWorks charted for its 600 banking clients during October. The most attacks — 775,000 — occurred on Oct. 6.

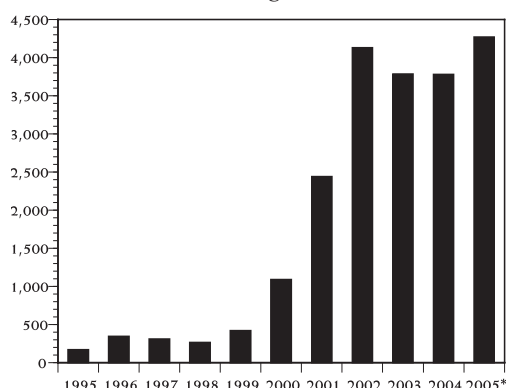


Source: SecureWorks

RISK MONITOR

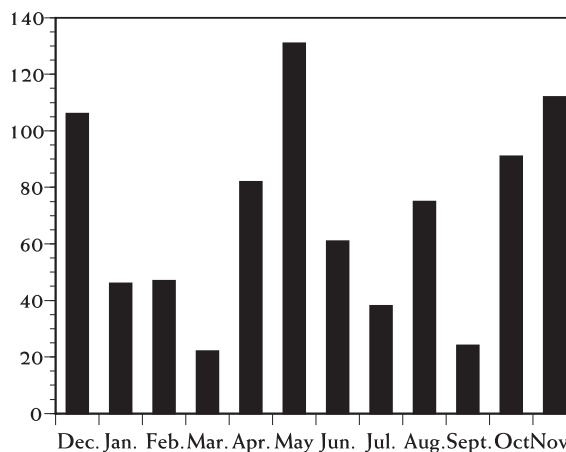
VULNERABILITIES REPORTED

through Nov. 30



Source: Cert Coordination Center

SDNS ADDED IN PAST 12 MONTHS



Source: U.S. Treasury Department

BREACH TRACKER

DATA BREACHES

Date Reported	Organization	Incident Description	Information Compromised/At Risk	Accounts Affected
Nov. 9	TransUnion Corp.	Stolen computer	Credit histories, personal data	3,600
Nov. 5	Safeway, Hawaii	Stolen laptop	Employee personal data	1,400
Nov. 4	USC Keck School of Medicine	Stolen computer	Student and patient personal data	50,000
Nov. 1	University of Tennessee Medical Center	Stolen laptop	Student and patient personal data	3,800
Oct. 21	Wilcox Memorial Hospital, Hawaii	Lost backup tape	Patient personal data	130,000
Oct. 15	Montclair State University	Online intrusion	Student personal data	9,100

Source: Privacy Rights Clearinghouse

TECH TRACKER

NEW PRODUCTS AND SERVICES

Company	Product/Services	Description	Price	Web Site
McAfee	AntiSpyware Enterprise	Antispyware protection	\$20 to \$25	www.mcafee.com
McAfee	Managed VirusScan plus AntiSpyware	Antispyware protection	\$28.56 to \$46.92	www.mcafee.com
Intellitactics Inc.	Security Assurance Metrics (SAM)	Security assessment system	\$35,000	www.intellitactics.com
Digital Resolve	Smart Cookie	Additional authentication	N/A	www.digital-resolve.net
Experian	Precise ID	Fraud detection, authentication	N/A	www.experian.com
Ping Identity	PingFederate v3	Identity federation server	free trial	www.pingidentity.com
Asigra	Televaulting for Enterprises Solution	Encryption	N/A	www.asigra.com
Experian	ASSIST//score	Regulatory compliance	N/A	www.experian.com
Memory Experts International	Outbacker MXP	Information management/protection	\$569 to \$699	www.memoryexpertsinc.com
Memory Experts International	Stealth MXP	Information management/protection	\$259 to \$479	www.memoryexpertsinc.com
RiskBusiness	Operational Risk Software Solution	Regulatory compliance software	\$343.56	www.riskbusiness.com
Tumbleweed	MailGate Appliance 3.0	Email security solution	\$5,200	www.tumbleweed.com
Network Chemistry	Rfprotect Survey	Wireless antivirus protection	\$2,999	www.networkchemistry.com

EQUITIES MONITOR

RECENT PERFORMANCE OF PUBLICLY TRADED INFORMATION SECURITY COMPANIES

Company	Ticker	Price 11/14	Price 10/19	4-wk ch(%)	P/E	52-wk High	52-wk Low	Shares Out.*	Market Cap.*	Average Volume
ActivCard Corp	ACTI	3.35	3.79	-11.61	N/A	9.75	3.21	43,940	147,199	238,600
Aladdin Knowledge Systems Ltd.	ALDN	17.82	16.01	11.31	22.6	32.12	15.78	14,350	255,717	232,000
Blue Coat Systems	BCSI	51.81	40.64	27.49	99.6	52.30	13.86	12,570	651,252	289,900
Brink's Co.	BCO	48.50	38.72	25.26	27.5	47.39	29.73	58,740	2,848,890	430,200
Check Point Software Technologies	CHKP	22.02	21.30	3.38	19.7	26.21	19.57	244,050	5,373,981	2,080,000
Cisco Systems Inc.	CSCO	17.40	16.91	2.90	20.0	20.35	16.83	6,280,000	109,272,000	53,800,000
Computer Associates International	CA	29.17	26.45	10.28	364.6	31.71	26.04	586,490	17,107,913	2,390,000
Entrust Inc.	ENTU	4.78	4.90	-2.45	53.1	6.63	3.28	60,000	286,800	450,700
Honeywell International Inc.	HON	36.08	34.18	5.56	23.3	39.50	32.68	842,760	30,406,781	3,880,000
International Business Machines	IBM	84.81	82.41	2.91	16.5	99.10	71.85	1,580,000	133,999,800	5,920,000
Internet Security Systems	ISSX	24.06	22.81	5.48	32.5	25.76	16.44	44,910	1,080,535	669,000
Magal Security Systems	MAGS	8.99	9.87	-8.92	47.3	15.25	7.82	10,370	93,226	51,300
Microsoft Corp.	MSFT	27.37	24.56	11.44	23.2	30.20	23.82	10,640,000	291,216,800	66,450,000
McAfee Inc.	MFE	29.50	30.10	-1.99	35.5	33.55	20.35	167,770	4,949,215	2,240,000
Napco Security Systems Inc.	NSSC	13.00	12.09	7.53	21.0	14.50	7.84	8,660	112,580	30,100
Novell Inc.	NOVL	7.85	7.15	9.79	8.6	7.78	4.94	381,990	2,998,622	5,440,000
RSA Security	RSAS	13.11	11.07	18.43	22.6	23.91	9.75	70,970	930,417	1,080,000
Safenet Inc.	SFNT	31.28	33.55	-6.77	347.6	38.22	25.30	25,160	787,005	430,600
Secure Computing Corp.	SCUR	14.16	10.95	29.32	27.2	14.23	7.38	31,190	441,650	500,200
Symantec Corp.	SYMC	19.60	22.10	-11.31	59.4	34.05	18.01	1,800,000	35,280,000	16,120,000
Trend Micro Inc.	TMIC	34.70	27.95	24.15	30.2	57.74	27.95	136,180	4,725,446	7,400
Tumbleweed Communications	TMWD	3.18	4.08	-22.06	N/A	4.40	2.01	49,090	156,106	296,000
VASCO Data Security Int'l Inc.	VDSI	12.40	8.93	38.86	88.6	12.05	3.40	35,940	445,656	551,900
VeriSign	VRSN	23.52	20.60	14.17	22.8	36.09	19.01	257,230	6,050,050	5,240,000
Websense Inc.	WBSN	64.62	52.91	22.13	44.3	63.67	44.01	23,800	1,537,956	560,400
Zix Corp.	ZIXI	1.86	2.01	-7.46	N/A	5.52	1.80	40,940	76,148	293,800

*in thousands; greatest gainer by percentage change in box

BOARD OF ADVISORS

CATHERINE A. ALLEN
Chief Executive Officer
BITS

JAY JANNISE
ISO/IT Manager
Premier Commercial Bank

SERGIO PIÑON
Senior Vice President
MasterCard

ERIK STEIN
Director, Fraud Prevention
and Investigation
Countrywide Home Loans

JAMES COWING
Senior Director
Digital Resources Group

ERWIN MARTINEZ
Chief Information Officer
Tamalpais Bank

JEFFREY B. RITTER
Attorney at Law
Kirkpatrick & Lockhart
Nicholson Graham LLP

KELLY WILLIAMS
Chief Information Officer
First Franklin Financial

ABBY HOSSEIN
Vice President,
Enterprise Infrastructure
Option One Mortgage

JIM MORRELL
VP Information Systems
iQ Credit Union

PAT RUCKH
Executive Vice President and
Chief Technology Officer
First Horizon Corp.

The Board of Advisors for *Bank Security News* provides insights and advice that help shape the scope and coverage of each issue.

The opinions expressed in *Bank Security News* are not necessarily shared by the board members nor their employers.

Register with BankNet 360 by
December 31, 2005 to be
eligible to win a prize.



The One Path to Financial Services Wisdom: BankNet 360.com

You can easily waste hours clicking from site to site for news on financial services. And even then, it's hit or miss — especially when you are checking for the latest buzz. You have more important things to do than google your time away.

What you need is a comprehensive, 360-degree look at everything online related to banking and financial services, updated to the moment. What you need is BankNet 360.

With proprietary technology and a sophisticated team of researchers, BankNet 360 uncovers the market intelligence you need to make smart business decisions. Choose from nearly 100 email alerts on every conceivable topic in banking, and access the information any way you'd like — even by RSS, the hot new technology for getting news online. Plus, you can quickly and effectively customize the site so you see only the news that matters to you most. And best of all, it's free. So stop clicking. Sign up for BankNet 360.



Get your 360 degrees. Join BankNet 360 today.

www.BankNet360.com