

Financial Alert

Management & Compliance Solutions for Financial Institutions

August 2001

Follow simple steps to boost Internet security

In the April *Financial Alert*, Jerry Lowrance, Springfield, discussed Internet security for financial institutions. In the accompanying article, managing consultant Frank Vukovits explores ways to further safeguard your customers' information.

by Frank Vukovits, Indianapolis

The growth of electronic commerce in a networked computer age raises new security dilemmas for financial institutions. Customers want round-the-clock Internet access to accounts, but they also demand more privacy and confidentiality of financial records.

These demands seem to conflict, because 24/7 Internet access opens new portals for serious security breaches. Consider the facts:

- ▲ Recent FBI investigations revealed several organized hacker groups from Eastern Europe had penetrated U.S. e-commerce computer systems to download proprietary information, customer databases and credit card information. In some cases, the information is sold to organized crime groups.
- ▲ The Computer Emergency Response Team at Carnegie Mellon University reports an estimated 21,000 attacks on web sites last year—a tenfold increase in just three years.

Many intrusions are internal. A

survey conducted by the Computer Security Institute and the FBI reported 71% of respondents detected unauthorized access to computer networks by their own employees.

Information is goal

Hackers, internal or external, rarely try to alter records. They're after confidential financial information, such as credit card numbers, account numbers, personal information and financial worth.

Consumers know the value of personal information, and they want it protected. Congress responded with the Gramm-Leach-Bliley Act of 1999 (GLBA).

GLBA outlines procedures designed to help you protect the security of customers' financial information. This involves more than disclosing your privacy policy to customers annually and offering an "opt-out" option.

It involves an integrated information security program in your institution and recommends using an independent third party to test key controls within the information security system before your next regulatory examination.

In short, do everything necessary to secure customer information from loss through theft, acci-

dent, acts of God, lax procedures, inattention to detail, entrusting it to the care of untrained personnel, leaving it unguarded, neglecting to account for it, forgetting where you put it and allowing unauthorized access to it.

Most hacks are preventable

Most security breaches are preventable with simple precautions. Industry experts estimate as many as 80% of successful hacker attacks could have been prevented through these simple steps:

Step #1: free patches slow hackers

When hackers detect vulnerability in corporate software, they share the information among themselves, usually via the Internet.

Software suppliers develop upgrades to "patch" these weaknesses. Licensed users of their programs can download these patches, posted on the Internet, free. Users often neglect to follow the postings and don't download the patches.

It is your system administrator's responsibility to keep your software—including the firewall—upgraded. This requires proactive daily checking for system patches. Depending on the number of software programs running in your sys-



tem, it's not uncommon to have several patches a week to download and install.

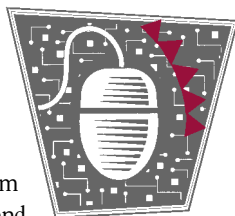
Hackers are up to date. Your institution should be, too.

Step #2: password protocols

Security surrounding passwords is often lax. Passwords should combine numbers and letters. Employees **continued on page 4**

In this issue

- ✓ Implementation key to profitability measurement
- ✓ ICBA, BKD co-author community bank survey
- ✓ BKD and Olive LLP merger enhances client services
- ✓ Brintech, BKD team to offer banking technology services
- ✓ NACHA changes require compliance updates.



Have you implemented profitability measurement?

by Carole Tanner, Indianapolis

Profitability measurement in financial institutions has become a necessity.

After months of planning for their measurement system implementation, many financial institutions fall short in the most critical and often most difficult phase: execution.

Typically, financial institutions view implementation as all the necessary steps to get the system running.

Something significant is missing from this line of reasoning. Successful implementation of profitability measurement requires steps before and after what is typically referred to as implementation.

Strategic & tactical planning

One frequently overlooked process is one of the most critical: a review of the financial institution's corporate strategy and the creation of a quantifiable strategic plan.

Developing this plan takes a lot of work. Failure here can lead to overall failure. The development process answers why you need a profitability measurement system, exactly what you intend to do with it and what results you expect.

If this process points to a lack of management or board support, financial resources or human talent to execute strategy and/or an unwillingness to hold and be held accountable, then don't buy the system.

Cultural (r)evolution

The second most frequently overlooked process involves establishing a solid foundation for awareness, education, acceptance, use

and ultimately an understanding of the rewards of using a profitability measurement system with your employees.

Dispel the myths

During the initial phase of profitability measurement system deployment (system creation), it's crucial to dispel the following myths that surround profitability measurement:

- ▲ Financial institutions will use profitability measurement as the only measure of customer value
- ▲ The measurement of profitability will segment customers into "good" and "bad" groups
- ▲ Financial institutions will compromise service quality for those who don't contribute profits

The facts don't support these myths. If used properly, customer profit contribution will be one of many factors to measure customer value. Profitable and unprofitable designations reflect the failure of the financial institution to match the right products with the right customers.

Profitability measurement offers an objective standard by which to measure service quality and optimize products to derive mutual benefit. It should be viewed as a means to improve service quality and customer satisfaction.

Identify early innovators

To begin laying the basis for employee acceptance, identify those who assume additional responsibility, readily accept change and have superb customer relation skills.

Show these innovators what the system does and doesn't do and how it can have a positive impact on customer service and profitability.

Provide them with predefined

marketing initiatives that support corporate strategy and make them responsible for executing those initiatives. Supply the tools to request information and measure results of their efforts. Communicate their efforts and results to the entire organization.

Involve customer service staff

After your early innovators are successful with the system, it's time to implement the program throughout the organization. Keep these things in mind during this phase of the project:

- ▲ Communicate corporate goals and measurement techniques
- ▲ Reinforce results of the early innovators and tie them to corporate goals with firmwide training
- ▲ Provide customized training for top management, marketing, finance and customer service representatives
- ▲ Provide the tools needed to request information and measure results
- ▲ Make profitability information a part of branch and personal goals, and tie it to individual compensation

Management's role

Many management teams fail following implementation because,

as excitement wanes, so does the allocation of resources and effort to the new system. To be successful, management must continually increase support of the new profitability measurement system.

Management must create an environment that requires use of the information at all levels.

Following are examples of ongoing utilization of information generated by the system:

- ▲ Assess strategic and tactical plans quarterly, measuring progress against baselines
- ▲ Fine-tune communication, marketing and sales promotions for best results
- ▲ Assess failure; if a tactic was correctly implemented yet failed, don't repeat it
- ▲ Continually tailor new initiatives based on trends in the customer base

Do it right

If your institution's profitability measurement system is correctly implemented, your customers should see an improvement in customer service and recognize your efforts to create products they need.

For more information on how to effectively implement and use profitability measurement, contact your BKD Financial Institutions Group advisor. □

BKD, ICBA to perform tech survey

BKD, through its alliance with Ininet Resources and in agreement with the Independent Community Bankers of America (ICBA) is co-authoring a survey to chart the use of technology by community banks.

The survey of ICBA's approximately 6,000 members will provide information about technologies these banks are using.

"The survey will determine which technologies community banks are currently using as well as those they plan to use in the future," says **Steven Nau** of BKD Technologies. Nau is helping to draft the questionnaire.

If you are a member of ICBA, watch for the survey soon, results of which will be published in the fall. □

Merger enhances services to financial institutions

In today's increasingly complex business environment, it's important to have a strong support team. Now with BKD on your side, you'll have even more support.

The June 1 merger of Baird Kurtz & Dobson and Olive LLP as **BKD, LLP** offers enhanced resources to help your financial institution succeed.

BKD Financial Institutions Group serves some 800 financial institutions clients in an 11-state region. This rich client pool, combined with the collective experience and skills of our team members, provide resources you will not find in local firms and at a price more competitive than that of international firms.

"The merger will enable us to get deeper and stronger in certain service areas where we were only one deep before," says **Jim Morris**, past industry director of Olive's financial services team.

Contact your BKD Financial Institutions Group advisor today or see our web site at bkd.com for

more information on these profit-enhancing services:

Outsourcing Solutions

- ▲ Internal audits
- ▲ Technology assistance
- ▲ Loan reviews
- ▲ Fixed asset administration
- ▲ Human resources consulting, including performance-based compensation plans
- ▲ Merger/acquisition services
- ▲ Strategic planning
- ▲ Internal control and fraud control reviews
- ▲ Due diligence
- ▲ Employee benefit plan administration

Regulatory Compliance

- ▲ Compliance monitoring
- ▲ Compliance audits
- ▲ Bank Secrecy Act independent reviews

- ▲ Community Reinvestment Act evaluations
- ▲ Fair Lending reviews
- ▲ Compliance program development
- ▲ Compliance policy and procedure development
- ▲ New product consulting and advertising reviews
- ▲ Customized compliance training for directors, officers and employees on topics ranging from Fair Lending to the Bank Secrecy Act
- ▲ Due diligence reviews
- ▲ Regulatory applications

Technology Services

- ▲ Assessment and strategic planning
- ▲ Selection
- ▲ Implementation and review
- ▲ EDP audits
- ▲ EDP control reviews

The united strength of

Olive
& **Baird, Kurtz & Dobson**

- ▲ Management information systems

Growth Enhancement Services

- ▲ Merger and acquisition
- ▲ Holding company formations
- ▲ IPO and stock conversions

Profitability Enhancement

- ▲ ProfitVision
- ▲ Analytical and planning services
- ▲ Asset/liability management
- ▲ Benchmarking

Tax and Assurance

- ▲ Tax services
- ▲ Audits
- ▲ Directors' examinations
- ▲ Trust department accounting services □

Brintech + BKD = enhanced technology services for financial institutions

BKD Financial Institutions Group leader **Don Hutson** announces a powerful technology alliance for the group's banking practice with Brintech, Inc., one of the nation's premier technology management firms.

Brintech, a technology management firm for the financial services industry founded by Harold Brewer, provides technology assessment and technology planning services.

"This alliance expands what we

can do for current clients and opens tremendous opportunities for growth," says Hutson.

The addition of Brintech's resources will deepen services currently offered by BKD Technologies, a division of BKD that provides information technology services to

financial institutions and other industries. The alliance will result in a five-fold increase in the number of technology pro-

fessionals dedicated to the BKD financial services client base.

"Our core services of technical assessment and planning, security planning and information technologies audits are now bolstered by telecommunications assessment and planning, Internet banking

solutions, call center strategies and marketing strategies including design development and support of web site applications," says partner **Jim Morris**, Indianapolis.

The alliance allows



infinet
RESOURCES

Independent Financial Institution Network

BKD and Brintech to collaborate on client engagements, providing clients with the best of both worlds: long-standing risk management and compliance expertise plus the skills and knowledge to implement today's leading technology.

This alliance is a result of BKD's affiliation with InFINet Resources, a network of independent CPA firms serving financial institutions. □

NACHA changes: are you in compliance?

by Rita Nelson, Kansas City

The National Automated Clearinghouse Association (NACHA) has made revisions to its 2001 operating rules and guidelines you should consider when planning your automated clearinghouse (ACH) audit this year.

Amendments may require internal updates

An amendment established a short-term rule, effective December 15, 2000, through March 14, 2002, that permits originators to use the prearranged payment and deposit format to truncate certain consumer checks. Customer service personnel may need additional training to answer customer questions resulting from this truncation process.

Two amendments to the NACHA rules became effective March 16, 2001. One established a shortened time frame for a financial institution to transmit a corrected return entry. Compliance with this rule may require a change in your internal procedures or ACH software.

The other amendment, effective March 16, 2001, created a new standard entry class code. Originators must use this code to identify con-

sumer debit entries initiated pursuant to an authorization obtained from the receiver via the Internet. The new web code addresses those unique risk issues inherent to the Internet environment.

Standard entry class code added

On September 14, 2001, an amendment modifying the NACHA rules will create a standard entry class code.

The new code must be used to identify single-entry consumer debit

entries initiated pursuant to an oral authorization obtained from the receiver via the telephone. This new rule streamlines the ACH authorization process by providing an alternative method for customers to authorize a one-time payment.

Whether you participate in the ACH network as an originating depository financial institution or receiving depository financial institutions, there are several unique implications with this new telephone-initiated entry code.



For additional information on how we can help you incorporate these amendments into your 2001 ACH audit, contact your BKD Financial Institutions Group advisor. □

Internet security. . .

continued from page 1

should memorize these and not share them with coworkers.

Password infractions commonly reported in security audits include:

- ▲ Systems that don't deny access when a user enters the wrong password three times. Hacker software will test every word in the dictionary as a password until one works. Passwords combining numbers and letters also will deny access to these hackers.



- ▲ Failure by the system administrator to change the default password on new network and/or firewall software. Hackers know the default passwords, too.

Path of least resistance

You could spend millions "beefing up" your security system. Still, a resourceful hacker can probably penetrate it.

Luckily, though, most hackers take the path of least resistance. If it's too much bother to penetrate your system,

they'll move on to an easier target.

You probably can't outsmart the hackers—but you can outsmart other institutions so the hackers won't bother you.

So what's the solution?

In the battle against unauthorized computer access, BKD Technologies is on your side. This division of BKD has solutions to strengthen your Internet security. For information on how we can help reduce your system's threats and vulnerabilities, contact your BKD Financial Institutions Group advisor. □

to How
Reach
BKD

P.O. Box 1900
Springfield, MO 65801-1900

inFinet
RESOURCES
Independent Financial Institution Network

bkd.com

For a complete list of our offices and subsidiaries and their contact information, go to bkd.com or call Director of Communications at 417 831-7283.

PRSRT STD
US POSTAGE PAID
SPRINGFIELD MO
PERMIT #801

Address Service Requested