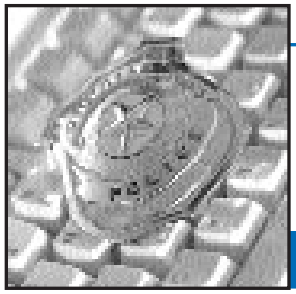
McGovern & Greene, LLP - Certified Public Accountants & Consultants - www.mcgoverngreene.com



Volume 2 No. 8 August 2003

# CYBER-CRIME FIGHTER

SUCCESS SECRETS FOR SECURITY MANAGERS AND INVESTIGATORS

## IN THE NEWS

### Gartner Alert—IDS Is Dead: Focuson Firewalls Instead

Intrusion detection systems (IDSs) have failed to provide value relative to costs and will be obsolete by 2005.

***Reason:*** IDS technology doesn't add the additional layer of security that its vendors promise. In many cases IDS implementation has proven to be very costly and completely ineffective. *Problems associated with IDSs…*

- False positives and negatives.
- Increased burden on the IS organization by requiring full-time monitoring (24 hours a day, seven days a week, 365 days a year).
- A taxing incident-response process.
- Inability to monitor traffic at transmission rates greater than 600 megabits per second.

***Better:*** Redirect infosec dollars toward firewalls that offer both network-level and application-level firewall capabilities in an integrated product.

***Key:*** Firewalls perform deep-packet inspection for content and malicious traffic blocking, as well as antivirus activities. They're the most effective defense against cyber-intruders on the network, and are becoming increasingly effective at blocking network-based attacks.

***Result:*** In coming years, firewall vendors will offer products that will replace IDS applications entirely.

***Cyber-Crime Fighter* source:** Richard Stiennon, Vice President, Research, Gartner, Inc., leading technology research and consulting firm, Stamford CT, www.gartner.com.

## IN THIS ISSUE



Craig Greene, CFE, *McGovern & Greene*

# PROTECTING TRADE SECRETS
## Practical Tech and Non-Tech Defenses

What are your organization's most valuable information assets and are they adequately protected? If you don't know, now is the time to find out, and if necessary take swift action.

***Important challenge:*** Though most trade secrets are now stored and protected electronically, some of the biggest risks of losing this information are non-technological. They include costly mistakes in granting access to secrets to the wrong people…negligence in training employees on what types of information to share and with whom…and similar "human error" vulnerabilities.

### TRADE SECRET VULNERABILITY IN PERSPECTIVE

An American Society for Industrial Security (ASIS) survey of Fortune 1,000 companies concerning trade secret theft found that these companies together lost more than $45 billion in a recent 12-month period. The biggest losses were in manufacturing and R&D.

***Important:*** ASIS also discovered that hackers and current or former employees are not always the greatest risk to an organization's proprietary information and intellectual property.

Very often, the criminals are outsiders who have a trusted relationship with the company—such as temps, Original Equipment Manufacturers (OEM)—companies that provide components, subassemblies, etc.—vendors and consultants. Too often, they are provided with access to company computer systems without any form of background check, reference check or on-site monitoring. (See page 4.)

### MAXIMUM SECURITY…

***Step One:*** **Perform an Information Asset Audit (IAA).** To determine what proprietary information is in your organization, consider such items as:

**Manufacturing…**
- Processes and methods
- Drawings and formulas
- Patents
- Vendor lists and pricing
- Marketing
- Customer information
- Future advertising campaigns
- Pricing schedules
- Contracts and bidding information

**Human resources…**
- Personnel files
- Health insurance files
- Payroll information

**Accounting and financial records…**
- Financial statements and supporting records
- Banking and finance info
- E-Commerce Applications
- Web site development code

***Important:*** In addition to this list, a trade secret may consist of any formula, pattern, device or compilation of information which is used in business…provides a competitive advantage…and is kept confidential.

***Step Two:*** **After installing and maintaining the necessary technological security measures for safeguarding trade secrets, determine whether your**

**non-technological systems for protecting these assets are adequate.** Is there a system in place for designating sensitive documents "Confidential," "Private" or "Sensitive"…and regularly updating the list of individuals with access to them?

***What to look for:*** Recurring "cracks" in your trade secret security systems.

***Step Three:*** **Immediately implement remedies for every vulnerability uncovered in the audit.** Tighten access rules and procedures governing trade secrets. Retain an outside information systems security expert to help with upgrading security technology.

## Sample of an Acceptable Computer Usage Policy

Scott Barman, a seasoned information security specialist, is among a small number of infosec experts who have published concise, easy-to-read and thorough sample computer usage policies for organizations. One of the most critical of such policies, which he calls, *Prohibited Activity and Use of Good Judgment…*

"Use of electronic communications to engage in any communication or action that is threatening, discriminatory (based on language that can be viewed as harassing others based on race, creed, color, age, sex, physical, handicap, sexual orientation, or otherwise), defamatory, slanderous, obscene, or harassing is prohibited.

Electronic communications shall not disclose personnel information without authorization. The destruction or alteration of electronic communications with the intent to cause harm or injury to the Company or an employee of the Company is strictly prohibited.

Electronic communications shall not be used for any illegal purposes or violate the intellectual property rights of others. Employees shall not break into the computers or intercept the communications of other individuals.

Employees will use the same good judgment to prepare electronic communications as they would use in preparing a hard copy of a memorandum. The content of electronic communications may have significant business and financial consequences for individuals of the Company and may be inappropriately taken out of context. Because of the ease of sending these documents, extra care must be taken to ensure that they are not sent hastily."

***Cyber-Crime Fighter*** **source:**

Scott Barman, who worked for NBC, Bell Communications Research (now Telecordia), TRW, other government contractors and many Internet companies. He is a contributor to the CISSP Training Guide and author of *Writing Information Security Policies,* New Riders Publishing, www.newriders.com. Scott can be reached at scott@barman.ws.

### LEGAL LIABILITY

The laws governing the protection of information assets generally fall into one or more of three categories:

•**Contractual restraints.** A company's case may rest on the fact that the information thief breached a confidentiality agreement or a non-compete agreement.

•**Fiduciary duties.** Management should aggressively train employees on how to weigh the appropriateness of releasing company secrets before doing so.

***Reason:*** Litigation can be initiated if a breach of this duty occurs during the suspected employee's tenure.

***Important:*** One-time training isn't enough. Regularly remind employees of their responsibility in this crucial area.

If the breach occurs after employment, your company should seek relief under the Uniform Trade Secrets Act (UTSA) or the Economic Espionage Act (EEA) (see below).

•**Trade secret law.** Though still somewhat vague, these statutes allow you to sue for punitive damages when trade secret theft occurs.

### TAKING ACTION

If you believe a trade secret has been stolen and you want to prosecute, the main laws on your side are the…

•**Uniform Trade Secrets Act (UTSA).** *Its scope focuses on…*

☐Acquisition by improper action such as a breach of duty or espionage, or by accident—provided that the "finder" wouldn't be prejudiced by the court granting relief.

☐ Unauthorized disclosure, such as transferring intellectual property to a competitor.

☐ Unauthorized use, for example, by an existing or newly formed competitor.

•**Economic Espionage Act (EEA).** This law addresses spying in order to obtain secrets. If intentional spying is suspected, the Act empowers the FBI to investigate suspects who steal secrets for foreign governments or economic gain.

***Important:*** The EEA also covers theft of commercial trade secrets by employees.

### BEST DEFENSE: FRONTLINE WORKFORCE

It may sound cliched, but because litigation is expensive and time-consuming,

*Continued on page 3*

**CYBER-CRIME FIGHTER**

***Success Secrets for Security Managers and Investigators***

*Editor*
Peter Goldmann

*Managing Editor*
Juliann Lutinski

*Senior Contributing Editor*
Ronald L. Mendell

*Associate Editor*
Barbara Wohler

*Design & Art Direction*
Ray Holland, Holland Design & Publishing



*Cyber-Crime Fighter* (ISSN1540-0891) is published monthly by White-Collar Crime 101 LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.cybercrimefighter.net. Subscription cost: $375/yr. Overseas: $397/yr. 

**Mission Statement**

*Cyber-Crime Fighter* provides information of maximum practical value to the community of organizations and individuals involved in preventing, detecting, investigating and prosecuting crimes committed by or against computers, networks and individuals.

This community includes law enforcement officials and regulatory officers at all levels of government, corporate security managers, business owners and managers, training professionals and educators.

The editors of *Cyber-Crime Fighter* gather and compile only the *most useful*, authoritative and timely information on all of the many facets of computer and Internet crime.

Comments, suggestions and questions are welcome. Please call us at 1-800-440-2261…or fax to 203-431-6054, or E-mail us at editor@cybercrimefighter.net.

*Continued from page 2*

and the outcome uncertain, it is more effective to prevent trade secret theft than to prosecute it after the fact.

Cliched or not, the statement is as valid as ever. To minimize your risk of litigation, maximize the security of your valued trade secrets.

***The key:*** Thorough and arduous employee training…

•**Avoid teaching as if the students were a blank slate.** Instead, determine what they believe they already know. Then fill in the blanks.

•**Simplify the law.** Make no distinction between information and documents that contain information. State that all company information is owned by the company and that employees are expected to abide by these rules at all times.

•**Emphasize that all information has competitive value and should be protected.** The company will determine how specific pieces of information are used and by whom…and will deploy the necessary technological safeguards to enforce this.

***Best:*** In-house seminars. Don't use the easy "solution" of bringing in legal counsel to preach to the masses. Instead, hold informal, but structured, discussions addressing what the employees know and what they might not. Reinforce the session with take-away reference materials.

### ALSO HELPFUL

•**Newsletters.** Distribute real-life case studies of trade secret theft, supplemented by analysis from company policy makers, and a restatement of the company's trade secret policy… with employee responsibilities.

•**Entrance, performance and exit interviews—**to determine what a person brings from previous employers. Assess the access an existing employee has to sensitive information and make adjustments if necessary. Evaluate and take precautionary measures concerning the risks of leakage upon an employee's departure. And—perform thorough computer security checks when an employee leaves, including changing passwords, removing appropriate files from the workstation, etc.

***Cyber-Crime Fighter* source:**

Craig L. Greene, CFE, CPA, partner in charge of Financial Investigation Services for McGovern & Greene, a Chicago-based corporate investigations and forensic accounting firm. He can be reached at craig.greene @mc governgreene.com.

**CYBER-LAW LESSONS**

# Here's What Can Happen When You Don't Secure Your Customer Data…

Companies that fail to take every possible measure to back up the claims they make about guaranteeing the privacy and security of personal customer information they collect in the course of conducting E-commerce could start paying dearly for their laxness. The penalty may be financial…or it may be in the form of lost customer confidence and costly paperwork.

***Pivotal case:*** Guess?, Inc., the parent company of Guess.com, the Web-based marketer of jeans and other apparel and accessories, agreed to settle Federal Trade Commission (FTC) charges that the Web site exposed customer credit card numbers and expiration dates to potential hacking, while giving its customers the impression that their personal information was completely secure.

According to a statement to consumers posted on the Guess.com site, "This site has security measures in place to protect the loss, misuse and alteration of information under our control"…and "All of your personal information, including your credit card information and sign-in password, are stored in an unreadable, encrypted format at all times."

***Problem:*** In February 2002, a 19-year-old visitor to the Web site, Jeremiah Jacks, discovered that Guess.com was open to a Structured Query Language (SQL) injection attack, which would enable a hacker to read in clear text more than 200,000 credit card numbers stored in Guess.com's databases.

***How it works:*** SQL injection attacks occur when an attacker enters certain codes into the target Web site that directs the Web application in use by the site to retrieve information from databases that support or are connected to the Web site.

***Example:*** An overnight package delivery company that offers a tracking feature for customers on its Web site. Legitimate customers are able to find the status of a shipment by entering the tracking number provided by the company at the time the order was entered. A malicious visitor to the site, however, could enter certain code into the tracking form that manipulate the site's software to pull up all of the shipment information in its entire database.

In the Guess.com case, the site was vulnerable to an attacker's manipulation of the site's application in order to gain access, in clear text, to every table in the Guess.com databases, including the tables containing the credit card information supplied by purchasers.

### WHY THIS IS IMPORTANT

According to E-commerce security experts, too many Web site developers focus only on the security issues of the operating system and Web server which the site will run on.

***Trap:*** While unplugged holes in these so-called Internet information security (ISS) functions can certainly be exploited by malicious attackers, IIS security is not the only part of Web site security.

Web applications connected to databases holding sensitive information have their own set of security vulnerabilities, such as SQL injections, that must be remedied.

***Critical lesson:*** Guess.com learned this the hard way when the FTC decided to investigate the security vulnera-

*Continued on page 4*

E-CASE STUDY

Alan E. Brill
CISSP, CFE, *Kroll Ontrack*

# Notes from the Kroll Casebook

## Who Has the Keys to the Kingdom?

It's no surprise to anyone who deals with white-collar crime and cyber-crime that the majority of incidents involve "insiders." But it can be easy to forget just how many categories of people meet that definition.

That became clear to us in a major case involving the theft of intellectual property.

Fortunately, our client—the victim—understood how important it was to preserve potential evidence when an information security incident occurred. So—when we worked through the computer log files and other digital evidence, we discovered that the incident traced back to a company that was a vendor of technology services to the victim company.

***Result:*** When we contacted the vendor we got an immediate denial of any knowledge of the incident.

***Problem:*** In further discussions with individuals close to the case, we discovered that an employee of the vendor company had quit his job with an attitude that clearly defined him as a "disgruntled worker."

That employee had worked on our client's account and knew the user ID and password to access the client's computer system.

Seeking to harm his former employer on his way out, he stole highly sensitive information that he believed would have significant value to competitors.

### COMMUNICATION BREAKDOWN

Unfortunately, the vendor saw no reason to inform our client that one of their recently departed employees knew our client's system password. In fact, the vendor had opposed our client's attempts to tighten controls on the account, claiming that it would be "harder for them to provide maintenance" if security was increased.

***Valuable lesson:*** Clarify what responsibility your vendors have for safeguarding the access that you have provided them to your system. Require them to specify what they are doing to protect your business from unauthorized use of the access you have provided.

If a security breach occurs, and it appears that the vendor has acted in an unauthorized or negligent manner, consult your attorney or legal department immediately to determine potential vendor liability.

### LESSONS FOR INVESTIGATORS...

When you investigate computer crime incidents, don't forget to find out which outsiders have been granted access privileges, and determine whether:

**Awareness and policy enforcement are vital keys to keeping effective control over access to critical information systems**

- There are appropriate security and control safeguards in place to adequately and consistently control the access accounts provided.

***Essential:*** Be especially vigilant about ensuring that you're using the best methods for authentication.

- There are rules in place requiring vendors to notify the customer if someone leaves their employ with knowledge of the customer's password…or if he or she is still employed but no longer works on the account. In either situation, the account access data should be immediately changed.
- The information made accessible to the vendor is appropriate to the situation. The vendor should have access to the information that it needs…but nothing else.

***The bottom line:*** While these are hardly complicated guidelines to follow, it is amazing how often they are overlooked. Awareness and policy enforcement are vital keys to keeping effective control over access to critical information systems.

***Cyber-Crime Fighter* source:**
Alan E. Brill, CISSP, CFE, Senior Managing Director, Technology Services, Kroll Ontrack, a division of the preeminent international investigative firm, Kroll Worldwide., New York, NY, www.krollontrack.com Alan can be reached at abrill@krollworldwide.com.

*Continued from page 3*

bility. The Commission proved that Web application vulnerabilities did exist despite the company's emphatic claims to customers that their personal identification information was fully secure.

***Outcome:*** The Commission ruled that Guess? did not adequately protect the personal information it obtained from on-line consumers. This inadequacy was the result of a failure to detect reasonably foreseeable security vulnerabilities and to prevent visitors from exploiting those vulnerabilities and stealing sensitive consumer data.

This constitutes unfair or deceptive commercial acts or practices in violation of federal law.

### SLAP ON THE WRIST... OR SETTING AN EXAMPLE?

Guess?'s settlement with the FTC prohibits the company from misrepresenting the extent to which it maintains and protects the security of personal information collected from or about consumers.

That may sound like an obvious and lenient penalty. And in fact, some infosec experts have criticized the deal as being just a slap on the wrist.

But the agreement also levies some extremely heavy administrative burdens on the company to document its compliance with the law. *Specifically, Guess?, Inc. must…*

- **Establish and maintain a comprehensive information security program…**and have the security program certified by an independent assessor with CISSP certification as meeting or exceeding the standards in the agreement within a year…and every other year thereafter.
- **For the next five years maintain—and produce to the FTC on request—**a copy of every print, broadcast, cable or Internet advertisement, promotion, information collection form, Web page, screen, E-mail message regarding its on-line collection, use and security of personal information about consumers.
- **Make sure that every Web page it maintains in compliance with the FTC has the full URL of the Web page** as well as all text and graphics files, audio scripts and other computer files used in presenting the information on the Web.
- **For the next three years, maintain all reports, studies, reviews, audits, audit trails, security assessments, risk assessments, policies, training materials, logs (from devices**

*Continued on page 5*

*Continued from page 4*

**that detect or prevent attacks such as firewalls and intrusion detection systems) and plans,** whether prepared by or on behalf of Guess?, relating to compliance with the FTC agreement.

### THE SANS ASSESSMENT

Allen Paller, director of research at the SANS Institute, summed up the FTC settlement as demonstrating that "there are legal consequences for organizations that have weak security. Tens of thousands of organizations doing business on the Internet are in the same (weak) position that Guess was in. Expect a surge of security audits… demand for better training for system administrators and application developers…and a quest for 'minimum standards of due care' in security."

***Cyber-Crime Fighter* sources:**

•Federal Trade Commission Complaint in the Matter of Guess?, Inc. and Guess.com, Inc., www.ftc.gov/os/2003/06/guesscmp.htm.

•Federal Trade Commission, Agreement Containing Consent Order, www.ftc.gov/os/2003/06/guessagree.htm.

•Allan Paller, Director of Research, SANS Institute, www.sans.org.

## Avoid the Guess? Trap

### E-Commerce Security: The Basics

*In announcing the Guess?, Inc. settlement, the FTC also published a short E-commerce security checklist for E-commerce companies…*

•Identify internal and external risks to the security, confidentiality and integrity of your customers' personal information.

•Design and implement safeguards to control the risks.

•Periodically monitor and test the safeguards to be sure they are working effectively.

•Adjust and update your security plan according to the results of testing, changes in operations or other circumstances that might impact information security.

•Carefully control the information handling practices of service providers and business partners who have access to your customers' personal information. If you give another organization access to your records or computer network, make sure they have good security programs too.

The Commission also recommends that E-commerce executives and administrators consult the two most widely respected summaries of Web site vulnerability…

•SANS Institute's *Twenty Most Critical Internet Security Vulnerabilities* (http://www.sans.org/top20/).

•Open Web Application Security Project's (OWASP) *Ten Most Critical Web Application Security Vulnerabilities* (www.owasp.org/).

## THE NEW CARD GAME

# STORED VALUE CARDS

## Major Convenience… Major Fraud Opportunity

Stored value cards—such as prepaid gift cards, so-called reloadable credit cards and similar alternatives to conventional cards—are rapidly gaining popularity among consumers. *Examples:*

•American Express's Cobaltcard

•Visa's VisaBuxx card

•MasterCard's PrivaCash card

•Numerous retailer and Internet-based private label and gift card programs.

***Result:*** A new level in payment card convenience for customers.

***Problem:*** Anything that makes life more convenient for consumers makes fraud easier for fraudsters.

***Good news:*** There are effective fraud detection and prevention systems for stored value cards. They are based on successful credit/debit card and Internet merchant fraud prevention systems.

### RISK MEASUREMENT

For card-issuing financial institutions, retailers and merchants, the fraud risks in stored value card programs occur in two main areas—account risk and transaction risk.

*The risks in both areas can be increased or decreased by…*

•**"Reloadability" of the card**—where a specific dollar amount is added to the card—say $100. Once it is used up another $100 can be added to the card and used. Each addition of funds is called a reload.

•**The diversity of merchant locations** that accept the card. The more diverse the channels—such as E-retail Web sites…retail stores…Voice Response Units (VRUs), etc., the more fraud is possible.

•**The anonymity inherent in card issuing distribution channels.** When fraudsters can be anonymous they are very happy. They purchase prepaid cards over the Internet with stolen credit cards, and then reload the prepaid cards with other stolen or generated card numbers.

### FRAUD PREVENTION FUNCTIONS

The secret of managing risk in a stored value card program—regardless of whether it is a reloadable account program or a disposable gift card program…or a hybrid of both—involves two distinct but integrated functions…

1) Account monitoring.

2) Transaction monitoring.

There are three main points in the issuance and use processes at which fraud detection systems are most effectively introduced…

•**Initial registration and funding of the account.** The initial registration activity has an account component—the registration or subscription…and a transaction component—the initial funding transaction.

Each should be scored independently and integrated with the other in order to successfully manage the risk of booking a fraudulent account.

***Key:*** The registration may look legitimate in that the identity theft is complete and convincing, even though it is totally fraudulent. Yet the funding component of the registration may be very high-risk—using card generation and number tumbling, or a high-risk combination of transactions.

The funding transaction risk may also be elevated due to an inconsistent combination of card issuer, E-mail address, IP address, billing address information, account registration address information, transaction timing, etc.

***Example:*** A "customer" may be funding a prepaid card with a card issued by a British credit card issuer…his or her IP address may be in Argentina…E-mail address may be anonymous…E-mail service is free, like hotmail…and the billing address

*Continued on page 6*

## NEED-TO-KNOW HOT LINE

# Overlooked Infosec Vulnerability: The Phone System

As if plugging the holes of vulnerability on computer systems weren't costing organizations enough money and aggravation, now there are reports of hackers increasingly using corporate phone systems (PBXs) to steal long-distance service, and to launch cyber-attacks.

Though "phreaking" is an old established pastime for hackers, according to the Department of Homeland Security as well as private-sector IT experts, there's a clear upward trend in hacking of corporate phone systems (PBXs), using them to steal long-distance service…as well as to steal data or launch other malicious attacks.

***Key:*** Newer PBX systems are directly interconnected with company network systems and are therefore used as conduits to proprietary data.

***Alarming:*** Since there are a relatively small number of players in the PBX equipment market, an attacker who takes the time to master two or three brands of PBX systems can have critical knowledge to attack more than 70% of all possible PBX targets.

*Other reasons for PBX vulnerability…*

•PBXs and peripherals have long useful lives, so many don't have state-of-the-art security features. Internal databases may even be unencrypted and easy to access and abuse.

•The people who manage PBXs are not always sensitive to security issues, so even obvious safeguards are sometimes missing.

•PBXs and peripherals are often managed off-site and almost all are set up for some form of remote access by users.

***Result:*** Hackers have little trouble finding these easily accessed entry points.

•PBX software upgrades are often made remotely, making it easy for hackers to intercept and corrupt them by installing Trojan horses.

•The telecom infrastructure is used by everybody—not just by trained personnel—which makes social engineering easier.

***Example:*** Calling a company employee and tricking him or her into revealing a password or other sensitive information.

***For preventive steps:*** Review the National Institute of Standards and Technology's *PBX Vulnerability Analysis* at http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf.

***Cyber-Crime Fighter* sources:**

•*Securing Your Switch,* John Jannschigg, Editor, Communications Convergence.com, www.commweb.com.

•*PBX Vulnerability Analysis* Institute of Standards and Technology.

•Robert Frances Group, Corporate IT consultants, Institute of Standards and Technology's PBX Vulnerability Analysis.

# Building a Culture of Information Security

Last year, the Organization for Economic Cooperation and Development (OECD), whose member nations include most of Europe, the US and several Asian democracies, published a document entitled *OECD Guidelines For The Security Of Information Systems And Networks.*

***Aim:*** To give member countries a blueprint for promoting a culture of security in the wired worlds of their corporate and individual citizens.

***Key:*** To do that, the document outlines nine broad principles for promoting a culture of security, including such imperatives as corporate responsibility for infosec…importance of doing risk assessments…enforcing ethics standards, etc.

***Important:*** The very first of the nine principles relates to awareness about the importance of security among companies, their employees and everyone else who relies on modern electronic applications in everyday life. *Specifics:*

"Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks.

[Institutions and individuals]should understand that security failures may significantly harm systems and networks under their control.

They should also be aware of the potential harm to others arising from interconnectivity and interdependency. They should be aware of the configuration of, and available updates for, their system, its place within networks, best practices that they can implement to enhance security, and the needs of other individuals and organizations."

Download the document at www.oecd.org/EN/search/0,,EN-search-43-nodirectorate-no-no-no-13,00.html.

*Continued from page 5*

information on the credit card may be in California. When the "customer" registers the prepaid account as if he lives in New York, you've got an ample number of inconsistencies to justify suspicion.

***Best fraud prevention method:*** Use a scoring process that evaluates not only the presence of the variables but the relationships between all of the variables. Expert rules are too fragile and one-dimensional to be economical or effective.

***Key:*** By analyzing the many sets of data involved in a transaction, the scoring process not only ranks the transactions and registrations by likelihood of fraud, it provides prioritization for operational evaluation.

**Anything that makes life more convenient for consumers makes fraud easier for fraudsters**

•**Monitoring of transaction activity on the card or account.** Transaction monitoring enables you to determine normal and customary activity for the issuer, the account and the fraudsters. It thus facilitates identification of unique activity by issuer, cardholder and fraudster.

***Key:*** Identifying and analyzing these patterns of activity allows the scoring system to assess risk across the card's entire transaction history.

A neural network transaction monitoring system provides the second layer of defense against fraud. This is important because no registration system can completely prevent fraudulent accounts from being opened.

This is especially true with the anonymity of Internet account registrations and funding transactions. The real-time application of the transaction scores allows card issuers to limit losses through the restriction of access to the remaining funds available in the account.

***Important:*** Any system that monitors stored-value transactions must be statistically sound to avoid the possibility of deploying subjective rules or policies that could result in discriminatory restrictions.

Neural network applications meet this requirement well because they are statistically based, empirically derived, provide a benign assessment of risk and do not introduce subjective components that risk discriminatory actions.

*Continued on page 7*

*Continued from page 6*

•**Reloading the account.** Each reloading of the account can and should be scored as a transaction using the records of all previous funding and transaction activity.

***Helpful:*** Activity-based profiles. They help to identify normal and suspicious behavior based upon issuer, account, "merchant" and previous funding activities.

Monitoring the account and all transactions is required to reduce the risk associated with this type of fraud.

***Cyber-Crime Fighter* source:**

Wesley Wilhelm, Director Risk Management, Fair Isaac Company, providers of predictive modeling, decision analysis, intelligence management, decision management systems and consulting services, San Rafael, CA. For information on available stored-value anti-fraud applications, contact Wes at WesleyWilhelm@fairisaac.com.

## Data Security Debate Goes National

As many had expected, the California law requiring companies to inform California customers when their personal identification information is compromised has become the potential model for a national statute requiring the same protection for all Americans.

California Senator Diane Feinstein introduced the Notification of Risk to Personal Data Act which, like its California forerunner that went into effect July 1, would require a business or government agency to notify individuals whenever there is a "reasonable basis to conclude that a hacker or other criminal has obtained unencrypted personal data maintained by that business or agency."

Already, business groups are warning that the bill will create confusion about who is responsible for reporting the information about breaches—merchants, credit card companies, government agencies, etc.

***For additional detail, visit:*** http://feinstein.senate.gov/03Releases/datasecurityrelease.htm.

*define as personal data an individual's Social Security number, driver's license number, state identification number, bank account number, or credit card number;

*subject entities that fail to comply with fines by the Federal Trade Commission of $5,000 per violation or up to $25,000 per day while the violation persists (State Attorneys General can also file suit to enforce the statute);

*and allow California's new law to remain in effect, but preempt conflicting state laws, so as not to put companies in a situation that forces them to comply with database notification laws of 50 different states.

# Inside Scoop

**From Cyber-Crime Fighter's files from the field…**

## *Better Whois Lookups*

The standard reference resource for finding out who owns a specific Internet domain name has for years been Whois, at www.networksolutions.com.

***Problem:*** While the domain registrar, Network Solutions, Inc.(NSI) has been the largest since the Internet became a household term, it no longer is the only one. There are now numerous domain registrars and since "Whois" belongs to NSI, getting the ownership and contact information for domain names *not* registered at NSI often doesn't work with Whois.

***Solution:*** www.betterwhois.com. It's a bit like Google in that it searches multiple domain registrars to find domain name ownership and contact data for names that are registered at Network Solutions as well as many other registrars.

***Cyber-Crime Fighter* sources:**

*The Fred Review*, on-line newsletter edited by James R. Richards, BSA Compliance Officer, Fleet Boston Financial and Ryan C. Perperas.

•Network Solutions, www.networksolutions.com.

•Betterwhois.com.

## *Temporary Employees: Potential Loose Cannons on the Infosec Deck*

If your organization relies heavily on temporary or contract personnel, it could be running a high risk of information security breach.

***Reason:*** Newly recruited temps are usually not made aware of the organization's information security policies…because most have no procedures in place to train temps in what is permissible and what isn't when using the organization's E-mail system and Web access.

***Result:*** Uninformed temps are more likely to inadvertently cause a security breach, than full-time permanent employees. Regardless of intent, if your organization can't prove that the individual was trained in how to comply with computer usage policies, costly liability problems could result.

The same applies of course when temps intentionally violate security policies and breach security measures. Not to mention the potential financial loss of such insider attacks.

***Solution:*** Formal and consistently administered security awareness training for all incoming and existing temporary employees on the company's infosec rules and procedures—before they are allowed to access sensitive systems. This can be done with either printed policy manuals…classroom-style orientation sessions…or a computer-based policy program where employees are required to read key policies and answer questions about them correctly before gaining access to the system.

***Cyber-Crime Fighter* sources:**

•Extend Technologies, a UK-based high-tech consulting firm and Morgan Cole, a prominent London law firm. The two organizations are partners in PolicyMatters, a software application for corporate policy implementation, www.policymatter.com.

•Cyndi Walsh, business training consultant, Wilson Learning, www.mccourtassociates.com.

## *Making a Dent in Software Piracy?*

The Business Software Alliance (BSA) announced the early results of its deployment of a new Web-crawl-

### Coming Soon in *Cyber-Crime Fighter*

•The new generation of WiFi security

•How Sarbanes-Oxley impacts IT security

•Best ways to guard against insider cyber-attacks

•How to keep infosec policies up to date

ing application that hunts down pirated software files and identifies their distributors.

The program, from New York-based Media Force, deploys intelligent agents to search the Internet for illegal software. It then displays the software and the distributor's IP address. BSA then contacts the Internet service provider (ISP), which in turn identifies the distributor and terminates the service.

***Impact:*** The MediaForce application has boosted the number of BSA notices to ISPs from 5,200 in all of 2001 to 8,500 in the first three months of deployment.

***How it works:*** The program finds unauthorized copies of software programs across popular file trading forums such as peer-to-peer systems, Internet Relay Chat (IRC) channels, Web sites, File Transfer Protocol (FTP) sites and newsgroups.

MediaForce's supporting case management tool tracks and archives notifications sent, monitors for compliance and flags non-compliant cases.

***Cyber-Crime Fighter* source:**

Business Software Alliance (BSA), a prominent international anti-piracy group with members including Microsoft, Apple, Adobe, Macromedia and Symantec, www. bsa.org.

## *On the Calendar*

**HTCIA Training Conference, October 20 through 22, 2003.** The High-Tech Crime Investigation Association (HTCIA) is holding its annual International Training Conference this October 20, 21 and 22 at the Embassy Suites Hotel Lake Tahoe Resort. *Training topics will include…*

•Counterfeiting—Internet and Computer Based

•Scams & Cons on the Net

•Financial Computer Forensics

•Computer Forensic Training—Certification-Associations

•Computer Forensics and High Technology Investigations—Testifying in Court

•Computer Forensics on a Budget

•Computer Forensic Units: Law Enforcement…Private Corporation …Task Forces

•Forensics with PDAs/Cell Phones/Blackberry Devices

***For more information visit:*** www. htcia2003. com/index.html.



## Reduce Infosec Risks in Operations

Operations security (OPSEC) is a term for the confidentiality of internal business processes and of sensitive information used in day-to-day operations.

If OPSEC is breached, the compromise can be used to gain unauthorized access to proprietary information such as client lists or source code…or to disrupt operations in a variety of different ways.

***Example:*** Fraudsters may call several employees throughout the organization, asking seemingly routine questions and in the process gathering key pieces of internal information—a name here, a unique business term there, etc. Before long, they have enough knowledge to impersonate an authorized computer or network user. *Self-defense:*

•Make sensitive information accessible only on a need-to-know basis.

•If someone you don't know is asking for internal information, verify their identity before complying.

•If the person doesn't or can't prove his or her need-to-know, the information is none of his or her business (literally). Cite company policy as your reason for not disclosing the information.

### SEMI-SENSITIVE INFORMATION

***Caution:*** Sensitive information can be deduced by gathering several pieces of public or unprotected information. These processes are called aggregation and inference. For this reason, semi-sensitive information must be protected as well. *Examples of semi-sensitive information include:*

•Organization charts
•Employee directories
•Store numbers
•Employee numbers
•Site locations
•Building blueprints
•Names of vendors or suppliers

***Helpful:*** Take a hard look at what outsiders could learn from public sources and from observing your operations. Web sites frequently are the source of unintentional information leaks.

Then fine-tune security policies and enforcement procedures to prevent distribution of semi-sensitive information you have identified.

***Cyber-Crime Fighter* source:** Gideon Rasmussen, CISSP, SCSA, Infostruct LLC, a Boca Raton, FL-based information technology consulting firm. Gideon can be reached at gideon@infostruct.net.