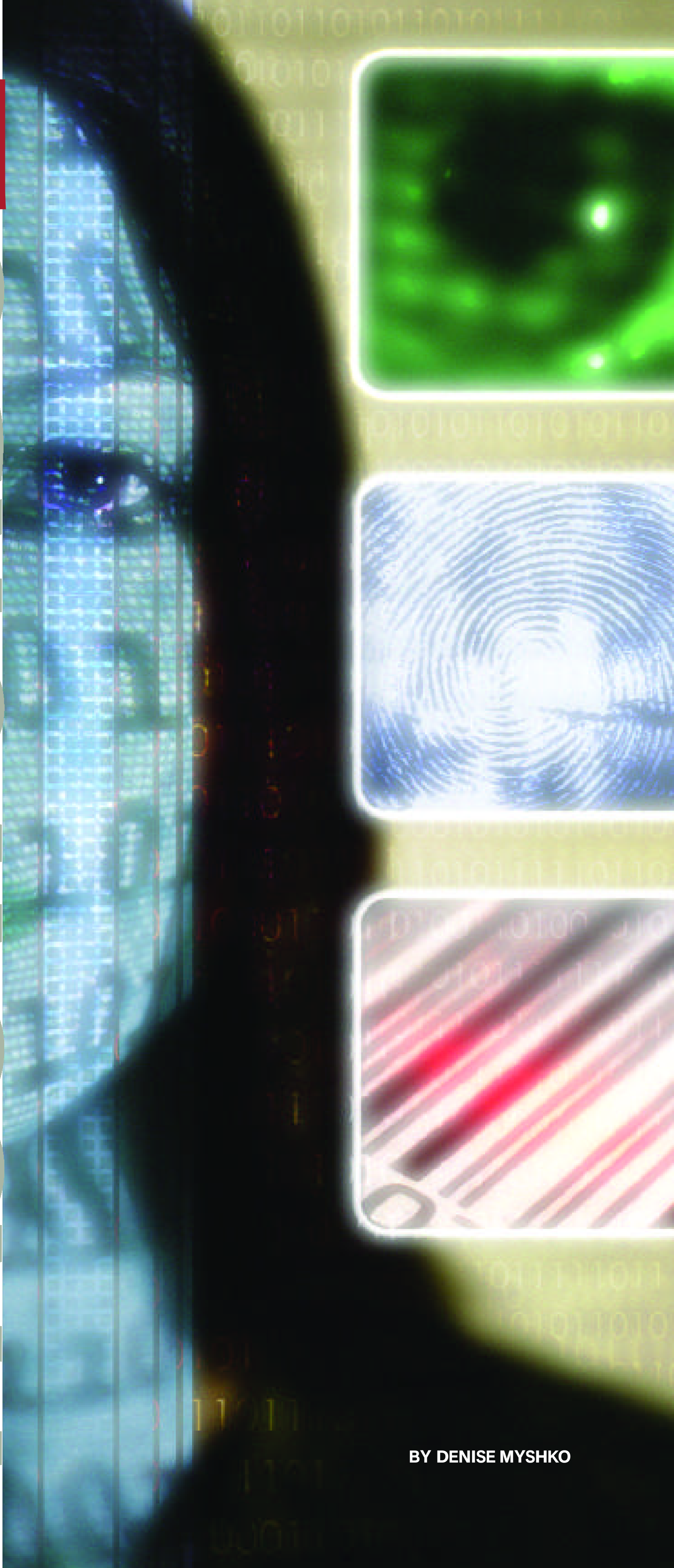
Beyond PASSWORDS

BIOMETRICS — TECHNOLOGIES THAT ALLOW PEOPLE TO BE IDENTIFIED BY FINGERPRINTS OR OTHER BIOLOGICAL MARKERS, SUCH AS IRIS SCANS — is receiving increased attention by companies in many industries concerned about security, not only for their premises but also for their information systems and the valuable, proprietary data within.



BY DENISE MYSHKO

Executives at Purdue Pharma understand all too well that the war on drugs isn't limited to heroin and cocaine. Since 2000, Purdue has been involved in controversy regarding the illegal use and abuse of OxyContin, an opioid agonist for the treatment of pain that the company introduced in 1995.

To enhance the security of its facilities, Purdue Pharma has implemented a biometrics technology — fingerprint readers that work with the company's swipe-card access system — for its manufacturing, packaging, and Q&A areas.

"Employees swipe their card, which is a 'smart card' that contains a fingerprint protocol," says Aaron Graham, VP of corporate security at Purdue Pharma. "The card tells the computer that I am Aaron Graham. Then I put my fingerprint on the reader. The fingerprint has to match the smart-card ID information for me to gain entry or access."

Biometrics — automated methods for recognizing a person based on physiological characteristics such as fingerprints, iris scans, voice and face recognition, hand and finger geometry, and handwriting analysis — has tremendous potential for the pharmaceutical industry. Not only can biometrics applications provide security to buildings but eventually the technology is expected to be used to protect IT systems and mobile-communications devices that house sensitive and proprietary information. Biometrics suppliers also say the technology can be applied to secure electronic signatures.

"Virtually all Fortune 500 companies have evaluated biometrics and have done some type of research," says Raj Nanavati, partner at International Biometric Group (IBG). "In a very broad sense, private-sector companies are piloting the technology for internal deployment or for their customers."

In the pharmaceutical industry, biometrics is very new. Some experts say barely 5% of the pharma industry has invested in some use of this technology and that is mainly for building security. Others say it may take at least five years for the technology to become more common in the industry. And even then, its acceptance is not assured.

"Right now, biometrics is viewed as an unnecessary layer of complexity," says Michael M. Breggar, DPM, global director of the life-sciences practice, Life Sciences and Healthcare Regulatory, at Deloitte & Touche. "If companies are comfortable with double-entry passwords, they may not make the investment in time, money, or training for biometrics. Additionally, when pharma companies apply any new application or a new technology, they have to go through a FDA-mandated process of system validation."

Still, for the heavily regulated pharmaceutical industry, biometrics has significant potential to increase the security of information across all aspects of the pharmaceutical industry — from manufacturing to research and development to physician interactions. Biometrics, for example, allows for an audit trail and better controls to remain in compliance with FDA electronic signature requirements for 21 CFR Part 11 and other applications that require authorization and verification of signatures.

"Pharma companies are very interested in the benefits biometrics has to offer from a logical access security perspective and a physical access security perspective," says Cliff Kittle, director of sales, emerging markets, at Saflink. "The pharmaceutical industry is probably the only industry that has felt significant impact from regulations such as 21 CFR Part 11, Sarbanes-Oxley, and HIPAA, and biometrics is an ideal technology for ensuring the integrity of information and meeting the requirements of all these regulations."

The technology also provides companies with better control over their systems.

"One of the problems that all companies face is that they can't consistently identify the persons within their systems," says Clyde Fritz, director of enterprise integration at Alliance Consulting. "Companies are spending millions of dollars trying to figure out a way to infer who is who across all their systems. With man-made identifiers, such as passwords, customer keys, and even names, companies have to infer who the person is. Because biometrics is not a man-made identifier, companies can automatically and immediately identify who is in a system."

AARON GRAHAM

I spent many years at the DEA as well as at the FDA. **WE RECOGNIZED THAT AS THE CRIMINAL ELEMENT GETS SMARTER, WE NEED TO DO WHAT WE CAN TO STAY AHEAD.**

ONE COMPANY'S EXPERIENCE

Purdue officials say within the next three

SETH BIRNBAUM

COMPANIES SHOULDN'T LOOK FOR ROI IN INFORMATION SECURITY BECAUSE THERE ISN'T ONE. Pharma companies have to understand where their risks are coming from and spend their dollars wisely to minimize them.

CLIFF KITTLE

The big payback of biometrics is going to come at the transaction level where audit trails are required. **COMPANIES NEED TO ENSURE THE AUTHENTICITY OF THE IDENTITY OF THE INDIVIDUAL WHO IS PERFORMING THAT TRANSACTION.**

to six months the company plans to implement a biometrics solution for its information systems. Additionally, Mr. Graham says biometrics solutions could be applied in the transportation security area to help determine access to containers and lockers.

"I spent many years at the DEA as well as at the FDA," Mr. Graham says. "We recognized that as the criminal element gets smarter, we need to do what we can to stay ahead. We manufacture OxyContin, a very valuable commodity, and we owe it to the public to make sure that the product stays where it is supposed to and is only distributed as intended. This is a commitment we have made to the public."

"Many companies that manufacture DEA-classed drugs or narcotics probably already have some type of biometrics technology to gain entry into their warehouses," Dr. Breggar says. "All companies have to be aware of the potential for theft, diversion, and corruption."

During 2000, the Drug Enforcement Administration (DEA) says there were 432 OxyContin theft and loss incidents, mostly from employee pilferage. OxyContin theft and loss incidents increased to 905 during 2002, with the majority of incidents from night break-ins, armed robberies, and employee pilferage.

Purdue has successfully defended itself against many lawsuits in state and federal courts that claimed OxyContin was unsafe or defective; had been improperly marketed by Purdue; or had caused the plaintiffs serious physical injuries, including addiction and death. In January 2004, the General Accounting Office (GAO) released the results of a two-year study to determine how OxyContin was marketed and promoted, what factors contributed to the abuse and illegal trafficking of the product, and what actions Purdue Pharma and others have taken to address the problem. The GAO stated that it could not assess the relationship between the growth in OxyContin prescriptions or increased availability with the drug's abuse and diversion.

Purdue has been working with state and federal authorities to ensure appropriate use and provide educational programs to patients about pain management. The company worked with the FDA to develop and implement a comprehensive risk-management program to ensure safe and appropriate use of OxyContin and to minimize its abuse. At a FDA advisory committee meeting Sept. 10, 2003, a FDA official acknowledged that Purdue's program is one of the best and most detailed plans developed to date.

Mr. Graham says senior management and employees alike have supported the use of the company's fingerprint system.

"We do a complete criminal background check on those employees who will deal with controlled substances," he says. "Our employees understand that to work here and handle controlled substances they cannot have a criminal record, and they understand what we have to do to protect and secure our company."

HEALTHCARE APPLICATIONS

The use of biometrics in healthcare is expected to be an area of rapid growth through 2005, according to IBG. Healthcare accounted for $43.3 million in biometrics revenue in 2002, and revenue from this sector is expected to reach $371 million by 2007. According to IBG, this anticipated growth can be attributed to legislative requirements, a heightened awareness of patient privacy, and the increased availability of personal medical information through remote channels. Areas of increased biometrics use include: the protection of patient data on internal networks, customer-facing applications, and the incorporation of biometrics functionality within software specifically geared toward healthcare. HIPAA, the Health Insurance Portability and Accountability Act, also will become a driver, since the law has required security standards for protecting health information.

The use of biometrics for PC/network security is expected to be one of the most rapidly emerging biometrics solutions over the next several years. It has already claimed a fairly significant portion of the biometrics marketplace, accounting for 19.1% of biometrics revenue in 2002, according to IBG. (See charts on page 42 for additional statistics.)

The biggest growth of biometrics will be in the area of government-related benefits, Mr. Nanavati says.

"This is a large sector where there is one organization controlling a process known to have a potential for fraud," he says. "While there may be some biometrics applications involving prescription refills, most applications involve hospitals and healthcare in general. For example, there is a large Medicare and Medicaid biometrics pilot program with 180,000 people in Texas."

Mr. Nanavati says most of the biometrics deployments in healthcare have been internal and relate to employee authentication for work station or facility access.

In the pharmaceutical arena, Saflink recently teamed up with Documentum to develop secure Web-top components targeted toward meeting the security needs of the industry. Saflink is developing a collection of components for secure authentication that are designed to be integrated into Documentum's browser-based content-management services.

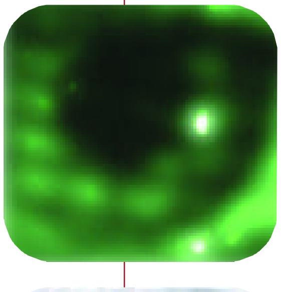
Saflink notes that through the use of biometrics, this framework is designed to guarantee the identity of a person participating in the creation and management of critical business documents and to provide the level of irrefutable identification required in highly regulated industries. Mr. Kittle says biometrics has significant benefit within pharmaceutical manufacturing.

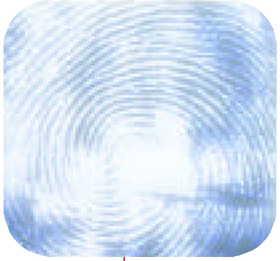
"A manufacturing execution system involves operators performing anywhere

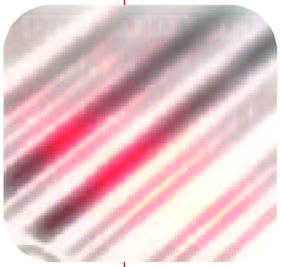
THE BIOMETRICS WORLD

BIOMETRICS SECURITY IS BASED ON A USER'S UNIQUE BIOLOGICAL CHARACTERISTICS: FINGERPRINTS, FACIAL FEATURES, VOICE, OR IRIS PATTERNS. THERE ARE NO PASSWORDS TO ENTER OR KEEP TRACK OF, THUS THERE IS NO COMPROMISE TO SECURITY, WHICH CAN HAPPEN WHEN USERS WRITE DOWN PASSWORDS TO REMEMBER THEM.

The use of biometrics technologies is not yet widely deployed, but is expected to increase in the coming years.







Of those who responded to a 2003 FBI and Computer Security Institute survey, just 11% have implemented these technologies. Those companies that do use biometrics are more likely to use other leading-edge technologies, including encrypted logins, digital IDs or certificates, and file encryption.

In 2003, biometrics industry revenue was $719 million, an increase of almost 20% from the year before, according to the International Biometric Group (IBG). According to these analysts, by 2008, revenue is expected to be $4.6 billion.

Researchers at IBG say this growth is predicated on the ability of the technology to address specific customer requirements and needs of identification and identity verification.

Growth will be driven by several factors, including the demand for centralized identity management solutions, incorporating both access control and logical access functionality; combination systems that provide authentication of the person and authorization to access secured resources; and increased use of wireless and remote devices to access sensitive networked or online resources. Fingerprint technologies are the leading biometrics technology in terms of revenue and are the most stable and proven biometrics operations.

The conceptual basis for fingerprint matching is well-understood and can be deployed effectively for verification of claimed identity.

The IBG report notes that because of competition in the fingerprint technologies market, there has been continual improvement in core technologies and this has led to cost reductions in certain market segments.

The use of biometrics for PC/network security is expected to be one of the most rapidly emerging biometrics solutions over the next several years.

According to IBG, PC/network security technology already has claimed a fairly significant portion of the biometrics marketplace, accounting for 19.1% of biometrics revenue in 2002. In 2006, revenue for this application is expected to approach $700 million.

Revenue generation in PC/network security is based on sales of hardware devices, most often $100 to $200 for fingerprint devices, and licensing of authentication software. For enterprise solutions, software packages ranging from $500 to more than $1,000 enable central storage, verification, and management of biometrics data, with additional per-seat license fees based on the number of end users.

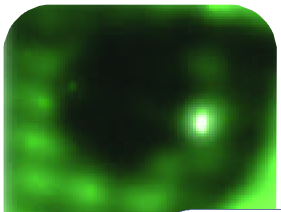
The first commercialized uses of biometrics technologies were to gain physical access to buildings. This has gained increased focus since the World Trade Center and Pentagon terrorist attacks. Since the attacks, there has been increased awareness of the vulnerabilities of sensitive sectors.

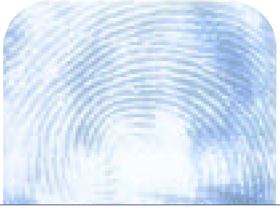
According to IBG, the government sector is the largest single user of biometrics, comprising 30% of revenue. By 2006, biometrics suppliers' revenue from this sector is expected to be about $1 billion.

Biometrics is one of several identity management technologies that the Department of Defense is using to protect its people, physical assets, and information. The Department of Defense has created the Identity Management Senior Coordinating Group (IMSCG) to provide cohesive departmentwide policy, requirements, strategy, and oversight to all programs involving the physical and virtual identities of its personnel.

The Department's Biometric Management Office (BMO) leads the effort to adopt and institutionalize biometrics technologies across the Department of Defense. As an element of the BMO, the Biometric Fusion Center (BFC) is establishing itself as the biometrics technology center of excellence for the Department of Defense. The BFC performs tests and evaluations of commercial off-the-shelf biometrics, supports the development of standards and performance measures, provides biometrics repository support as required, and provides technical implementation and integration support.

Additionally, the Department of Homeland Security uses biometrics in a wide variety of applications, including airport security, the adjudication of asylum claims, and for establishing and verifying the identity of illegal immigrants apprehended crossing the border.





BIOMETRICS INDUSTRY REVENUE

2002-2008

YEAR	PROJECTED REVENUE ($ ARE IN MILLIONS)
2002	$599.9
2003	719.0
2004	1,200.7
2005	1,847.2
2006	2,684.4
2007	3,682.7
2008	4,639.4

Source: International Biometric Group, New York.
For more information, visit biometricgroup.com.

BIOMETRICS REVENUE PROJECTIONS BY MARKET SEGMENT

SECTOR REVENUE ($ ARE IN MILLIONS)

	2003	2004	2005	2006	2007	2008
Law enforcement	$247.1	$326.3	$430.3	$544.5	$689.1	$839.6
Government	240.8	432.1	685.9	1022.4	1413.1	1779.1
Financial sector	48.3	93.6	159.5	236.4	324.7	405.5
Healthcare	26.4	49.1	80.3	118.4	159.9	196.9
Travel/ transportation	85.2	149.8	238.6	366.4	527.5	677.2
Other	71.3	149.7	252.5	396.3	567.7	741.1

Source: International Biometric Group, New York.
For more information, visit biometricgroup.com.

BIOMETRICS TECHNOLOGIES AND REVENUE PROJECTIONS

TECHNOLOGY REVENUE ($ ARE IN MILLIONS)

	2003	2004	2005	2006	2007	2008
Fingerprint	$198.0	$367.9	$582.9	$858.4	$1162.2	$1493.0
Facial recognition	50.0	114.2	228.0	417.0	622.1	802.3
Hand geometry	43.0	87.9	123.1	137.4	148.1	154.2
Middleware	48.0	79.8	131.5	208.6	306.5	396.7
Iris recognition	36.0	71.5	112.4	189.9	282.6	366.3
Voice	23.0	45.9	76.2	114.4	169.2	224.6
Signature	9.0	18.8	33.6	53.5	83.4	106.9
Multimodal	11.0	28.7	58.6	105.9	161.5	220.3
AFIS	312.0	414.6	559.4	705.2	908.7	1095.3

Source: International Biometric Group, New York.
For more information, visit biometricgroup.com.

between 300 and 600 transactions per operator per an eight-hour shift," he says. "If a company can reduce the time it takes to verify each transaction by 50%, it can realize significant production improvements. Biometrics can address 21 CFR Part 11 from an administrative perspective versus a user ID system. With biometrics, companies don't have to worry about someone using another person's identity."

Marc Diament, executive VP of business development at Net-Scale Technologies, agrees there is a growing application for biometrics for processes involving electronic signatures.

"In manufacturing, there is a lot of repetitive use of digital signatures, and there are a lot of paper processes," he says. "Instead of having employees sign and date everything, companies can use biometrics technology to digitally sign and date transactions. The fingerprint, essentially, is a signature."

He says the advantages to this are speed, security, and convenience.

"Employees can touch a fingerprint sensor and that fingerprint can be found and submitted 20 times faster than it takes to type in the information," he says.

As the move toward outsourcing continues to increase, Mr. Kittle says there are tremendous opportunities within the R&D arena.

"Companies that are outsourcing R&D have to be very comfortable with who has access to information and how that partner organization is securing the data," he says. "This is especially significant since it is often cheaper to steal research than to conduct it. This is particularly relevant in the pharmaceutical industry, where industry investment in R&D has grown from $1.3 billion in 1977 to $32 billion in 2002. The big payback of biometrics is going to come at the transaction level when an audit trail is part of the requirement. Companies need to ensure the authenticity of the identity of the individual who is performing the transaction, and biometrics is ideal, because it is based on a unique biological characteristic that can't be lost, stolen, or borrowed."

There are also obvious applications within pharmaceutical companies' information technology systems.

"To ensure security, companies enforce complex passwords with names, numbers, and weird characters," says Nicholas Stamos, VP of products and services and cofounder of Verdasys. "But as passwords get more complex people can't remember them, so they write them down and put them on a yellow sticky next to their computer."

Verdasys, a provider of security solutions, was founded by a group of individuals from a biotech company that averted a loss of its intellectual property.

"Employees had access to close to $100 million of chemical-structure information that we had derived from our research," says Seth Birnbaum, CEO and a cofounder of Verdasys, and founder of the biotechnology company Neogenesis.

"Three employees all ordered CD burners on the same day, which we thought was suspi-

LOSSES BY THE NUMBERS

2003 LOSSES BY TYPE
($ ARE IN MILLIONS)

Theft of proprietary info	$70,195,900
Denial of service	$65,643,300
Virus	$27,382,340
Insider net abuse	$11,767,200
Financial fraud	$10,186,400
Laptop theft	$6,830,500
Sabotage	$5,148,500
System penetration	$2,754,400
Active wiretapping	$705,000
Telecom fraud	$701,500
Unauthorized/insider access	$406,300
Telecom eavesdropping	$76,000

Source: Computer Security Institute, San Francisco.
For more information, visit gocsi.com.

cious," he says. "It turns out they wanted to start their own company. The loss of that information would have been strategically disastrous for Neogenesis."

The threat of theft, loss, misappropriation, or destruction of intellectual property is a growing problem for companies.

According to a September 2002 report by PricewaterhouseCoopers, the U.S. Chamber of Commerce, and ASIS Foundation, although 70% or more of the market value of a typical U.S. company is derived from its intellectual property assets, formalized valuation procedures exist in too few companies. Since the value is not well established, these assets are often not protected and this contributes to problems associated with theft of trade secrets and sensitive information.

Those surveyed by PricewaterhouseCoopers were likely to have experienced proprietary information and intellectual property losses of between $53 billion and $59 billion.

"For large companies, especially intellectual property intensive companies such as pharma, by far their most significant information-based loss is potential theft from insiders, people who are authorized to use their systems," Mr. Birnbaum says.

According to a 2003 FBI and Computer Security Institute survey, 56% of respondents reported unauthorized use of systems. The total annual losses reported in the 2003 survey were $201.8 million. (See chart on this page for more information.)

As in previous years, theft of proprietary information caused the greatest financial loss — $70.2 million, with the average reported loss being about $2.7 million.

Virus incidents (82%) and insider abuse of network access (80%) were the most cited forms of attack or abuse.

The greatest risk factors associated with the loss of proprietary information and intellectual property among all companies responding to the survey come from former employees, foreign competitors, on-site contractors, and domestic competitors, according to the PricewaterhouseCoopers survey. The most commonly cited areas of risk by companies that reported an incident: research and development (49%), customer lists and related data (36%), and financial data (27%).

Among all companies, increased legal fees and loss of revenue were the most serious outcomes from proprietary information loss. For large companies, those with revenue of more than $15 billion, loss of competitive advantage was the most serious problem.

Another area that is starting to raise a lot of interest is validating employee time and attendance, Mr. Kittle says.

"Fraud costs involving time and attendance are between 6% and 12% of an organization's annual payroll," he says. "Biometrics can eliminate 'buddy punching,' which is the main contributor to this type of fraud. Another 2% to 3% of annual payroll costs is related to administrative errors. Eliminating costs associated with these areas through an authentication process can save a company millions of dollars a year."

Biometrics technology can complement or replace keys, tokens, or badges. Revenue in this area is expected to grow from $90.9 million in 2002 to about $250 million in 2004 and is expected to account for 15% to 18% of biometrics revenue during the next several years, according to IBG.

TECHNOLOGY TODAY AND TOMORROW

Because fingerprint technology provides a strong balance between accuracy and convenience, it will continue to be the most commonly implemented biometrics solution.

NICHOLAS STAMOS

COMPANIES ENFORCE COMPLEX PASSWORDS. But as passwords become more complex, people can't remember them, so they write them down and put them on a yellow sticky next to their computer.

In addition, as remote access to personal data becomes common, fingerprint technology embedded in keyboards and peripherals will be used to secure online access, IBG researchers say.

Mr. Fritz says an application for fingerprint technology involves sample drops by field-force sales representatives. He notes that some high-end laptops already include fingerprint recognition systems.

"The challenge that pharmaceutical companies will have is how to get doctors to agree to have their fingerprint encoded in a database where the information can be recorded and referenced; this is especially challenging at a time when people are nervous about privacy issues," Mr. Fritz says.

IBG researchers also predict that biometrics will be used in kiosk-based healthcare applications for prescription disbursement and information retrieval.

MARC DIAMENT

WE HAVE EXPLORED RESISTANCE TO BIOMETRICS IN THE WORKPLACE WITH REAL USERS. Our results suggest that people are excited to use this technology and that they are not overly worried about having their fingerprints scanned.

The University of Alabama Integrated Biometrics Lab is developing software for the integration of fingerprint and voice and face recognition. The lab is developing these applications for use by retail and travel segments, as well as for various government agencies.

"As an improvement to unimodal biometrics applications such as a fingerprint verification system, multimodal recognition systems provide increased accuracy and are less susceptible to fraud," says Reza Adhami, Ph.D., professor and chairman of the department of Electrical and Computer Engineering at the University of Alabama in Huntsville. "Multimodal biometrics recognition systems combine the information from two or more independent biometrics devices."

According to Dr. Adhami, the idea is to ensure authentication by incorporating voice and/or facial recognition with a fingerprint system providing biometrics diversity in the event that the result of the fingerprint verification is borderline.

"UAH is currently collaborating with PERL Research on just such a system," he says.

According to IBG, multimodal solutions that require the submission of more than one biometrics characteristic, such as fingerprint, face, voice, and iris, are expected to comprise an increasing percentage of the biometrics industry, but will remain a minority.

At the retail level, Dr. Adhami says fingerprint technology used in conjunction with smart cards is becoming more practical.

"The goal is to enable credit-card holder identity authentication by providing a fingerprint identification system on a credit card, which will allow fingerprint comparison to that of the card holder scanned at the time of purchase," he says. "This type of authentication would result in a huge reduction in credit-card theft."

He says annually about $1 billion in losses can be attributed to identity/credit-card theft and about $1 billion in fraudulent ATM withdrawals.

HURDLES AND OBSTACLES

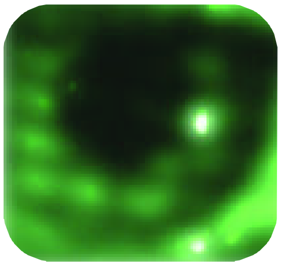
Cultural acceptance, Mr. Fritz says, is likely to be a significant hurdle for the adoption of biometrics, even though the information is encrypted.

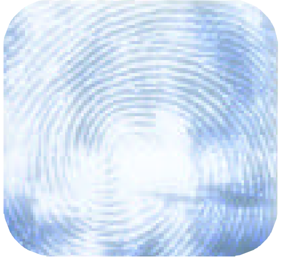
"A fingerprint reader creates a template that is a measurement of about 25 to 30 unique points in an individual's biometrics," Mr. Kittle says. "The systems store this template in a secure area, which is encrypted and saved to an area of the customer's choice. There is no way to reverse engineer the template to recreate that fingerprint."

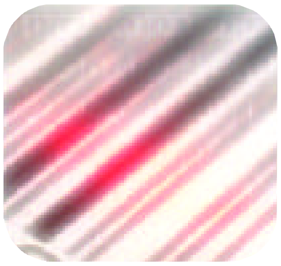
Until recently, a lack of standards for biometrics had been an issue, but several developments are under way to address this concern. The Commerce Department's National Institute of Standards and Technology (NIST), in cooperation with the American National Standards Institute (ANSI), has developed a uniform way for fingerprint, facial, scar, mark, and tattoo data to be exchanged between different jurisdictions and between dissimilar systems made by different manufacturers.

Many companies have developed software that uses complex algorithms for facial recognition. NIST researchers have designed tests to measure the accuracy and reliability of these software programs in matching facial patterns, using both still and video images.

NIST has worked in partnership with U.S. industry and other federal agencies to establish formal groups for accelerating national and international biometrics standardization. Two recent additions are the Technical Committee M1 on Biometrics, started in November 2001 by the executive board of the International Committee for Information Technology Standards (INCITS), and a new subcommittee on biometrics (the Joint Technical Committee 1 SC 37 - Biometrics) created in June 2002 by the International Organization on Standardization (ISO).







Additionally, the Biometric Consortium serves as the federal government's focal point for research, development, testing, evaluation, and application of biometrics-based personal identification and verification technology. The consortium now has more than 900 members, including 60 government agencies.

NIST has collaborated with the consortium, the biometrics industry, and other biometrics organizations to create a Common Biometric Exchange File Format (CBEFF). The format already is part of government requirements for data interchange and is being adopted by the biometrics industry.

COSTS AND ROI

In terms of cost, biometrics is like any new technology, Mr. Kittle says. Over time, prices will continue to go down.

"There are a number of different studies that have evaluated what the associated costs are with ID and passwords," he says. "The IDC estimates it costs companies between $200 and $300 per year, per user, for help-desk costs because of password resets. If a company has four applications, a user is going to spend about 44 hours a year logging onto those applications. The average user has between six and 12 passwords. In a manufacturing environment, biometrics can cut down the time to perform those transactions by 50%. A person can be 30% more productive."

Mr. Birnbaum, however, says it is unwise to try to pin down ROI for a security system.

"We encourage our customers to do a risk-management analysis," he says. "We advise them not to look for ROI in information security because they just won't find it. Pharmaceutical companies have to first understand where the greatest risks are to their information and then spend their dollars wisely to minimize the threat."

If pharmaceutical companies could find an economical way to mesh biometrics with standard systems, they could save millions of dollars every year, Mr. Fritz advises.

"The ROI from biometrics comes into play when we evaluate what companies are spending day to day to infer who is who; the amount of money that is spent on this is mind boggling," he says. "If companies can replace inference with a biometrics identifier, we can begin to calculate this tremendous ROI."

At this point, he says, the cost of reengineering systems is significant, but it is possible to mesh the two worlds through the use of an intelligent filter.

"When the biometrics system scans someone and recognizes that person, the information is carried to that filter, which then searches the company's other systems to find information about who this person is to the enterprise," Mr. Fritz says. "The value from biometrics comes from the ability to relate the scan to all of a company's back-end efforts and this comes from investing in the intelligent filter."

"Implementing a biometrics technology involves changing processes, not just changing technology," Dr. Breggar says. "The business case needs to examine what the change in technology means to the company, what the change in process is going to mean for employees and customers, as well as the costs involved."✥

PharmaVoice welcomes comments about this article. E-mail us at feedback@pharmavoice.com.

DR. MICHAEL BREGGAR

Biometrics will begin to creep into the life-sciences sector, but significant movement is not going to happen for at least five years.

BIOMETRICS PRODUCTS HAVE TO BECOME EASIER TO USE AND LESS EXPENSIVE.

Experts on this topic

REZA ADHAMI, PH.D. Professor and Chairman of the Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, Ala.; The Department of Electrical and Computer Engineering offers undergraduate engineering programs, master's degree programs, and Ph.D. programs in several areas of engineering, including computer engineering, electrical engineering, software engineering, photonics engineering, and optical science and engineering. For more information, visit uah.edu.

SETH BIRNBAUM. CEO and Cofounder of Verdasys Inc., Waltham, Mass.; Verdasys provides a class of risk-management solutions focused on the uncountered threat from authorized users or insiders. For more information, visit verdasys.com.

MICHAEL M. BREGGAR, DPM. Global Director, Life Sciences Practice, Life Sciences and Healthcare Regulatory, Deloitte & Touche LLP, Glen Mills, Pa.; Deloitte & Touche LLP's Health Care & Life Sciences Practice, with U.S. headquarters in New York, works with clients to shape the evolution of the industry. For more information, visit deloitte.com/us/healthcare.

MARC DIAMENT. Executive VP, Business Development, Net-Scale Technologies Inc., Morganville, N.J.; Net-Scale Technologies specializes in innovative, high-quality software design and development for the telecommunications, healthcare, manufacturing, government and defense, and customer-relations management industries. For more information, visit net-scale.com.

CLYDE FRITZ. Director of Enterprise Integration, Alliance Consulting, New York.; Alliance Consulting is an information technology consulting firm that delivers business-driven solutions. For more information, visit alliance-consulting.com.

AARON GRAHAM. VP of Corporate Security, Purdue Pharma LP, Stamford, Conn.; Purdue Pharma is a privately held pharmaceutical company known for its pioneering research on chronic pain. For more information, visit pharma.com.

CLIFF KITTLE. Director, Sales, Emerging Markets, SAFLINK Corp., Woodstock, Ill.; SAFLINK, with headquarters in Bellevue, Wash., offers software solutions designed to protect intellectual property, secure information assets, and eliminate passwords. For more information, visit saflink.com.

RAJ NANAVATI. Partner, International Biometric Group LLC, New York; IBG is an independent integration and consulting firm, providing a broad range of services to government and private sector clients. For more information, visit biometricgroup.com.

NICHOLAS STAMOS. VP, Products and Services and Cofounder, Verdasys Inc., Waltham, Mass.; Verdasys provides a class of risk-management solutions focused on the uncountered threat from authorized users or insiders. For more information, visit verdasys.com.