Appeared in the Fall 1997 edition of BioTech News
Gene Tucker, CPP, CFE, CBCP

PROTECTING YOUR INTELLECTUAL PROPERTY

BANK EMPLOYEE WALKS OUT DOOR WITH $1.5 MILLION DOLLARS.

A longtime, trusted employee of the First Irrational Bank disappeared Friday with over one and one half million dollars in cash recently transferred to the bank from the National Reserve. It is believed the employee fled to Mexico. Along with the local police, the Federal Bureau of Investigation has joined forces with the State Department and Interpol in an attempt to locate this individual. Florence Nightinjail, Special Agent at the Washington, DC office of the FBI stated 'We expect to include the suspect on our 10 Most Wanted List soon.' Senator Don Nothing, in his statement calling for a Congressional investigation said 'We expect many heads will roll when this matter is resolved.' For a description of the suspect, tune in to the television show 'America's Most Wanted' this Friday.

Does this story sound plausible? You may agree that, although the likelihood of such a large theft of cash from a financial institution is minimal, the response is typical. But what would happen if we changed the story line to read: **Disgruntled employee sells bioactive proteins worth $250 Million in research and future sales to foreign drug manufacturer**? First of all, we would probably never see the headline. One reason is the victim company never knew the proteins were missing until it was too late.

We devote huge resources to protect relatively small amounts of assets in our local banks. However, the company jewels are often given away by good meaning employees trying to contribute to the academic culture they have shared all their career. These treasures are misappropriated by employees who feel they have a right to their research, or they are stolen by employees bent on revenge or greed. Sophisticated corporate intelligence departments can dupe even the most trusted employee into giving away vital information they would never tell their spouse. With the fall of the iron curtain, the same agents that used to target our military secrets are now focusing their national resources on our industries, in particular biotechnology. Our industrial secrets will give their countries an economic strength that military power could never achieve. The use of diplomatic cover and foreign companies to exploit joint ventures are still common practices. Even our 'friends' - France, Israel, Japan, Switzerland, and others actively seek our technology and research, often by less than noble means.

Sound farfetched? Right now in the Silicon Valley County of Santa Clara California, the District Attorney is prosecuting 7 trade secret theft cases. Not all of these cases are tied to international intrigue. The American Society For Industrial Security estimates that in 1993, 57% of trade secret losses (70% if contractors and vendors are included) involved internal theft. In fact, most of Santa Clara County's 29 cases in the last five years involved a disgruntled employee.

Can anything be done to protect your secrets in the face of these exposures? Following even the simplest security rules can prevent the loss of millions of dollars in research, market position, and future sales.

- Identify your trade secrets or proprietary information. Trade secrets can include the formula to a new product, laboratory notebooks, a unique processes or equipment, test results, client or market lists, etc.

- Take active steps to protect this information. If you use the courts for relief, you face the danger that the jurisdiction may decide information was not technically a secret because you did not take sufficient steps to protect it.

- Conduct pre-employment background investigations on potential employees. Three cases under investigation in Santa Clara County in the month of July 1995 involve employees who were inserted into the company with the specific intent to remove proprietary information. Know who you are giving access to your secrets and weed out those employees who have the potential to destroy your business.

- Improve access control to the facility, both externally and internally. The level of access control is often used by the courts to evaluate the degree of protection given to trade secrets.

- Improve the physical security of the building or site. Lighting, physical barriers, environmental design, alarms, and CCTV are basic methods used protect documents and information. Use independent security consultants to help determine what protections are appropriate for your site.

- Actively prosecute employees who steal intellectual property. Many employees who commit this crime do not think it is wrong or think nothing would happen to them if they are caught.

- Have employees sign a non-disclosure agreements and place brief nondisclosure warnings on visitor and contractor sign-in registers.

- Consider exiting employees from the company as soon as they give notice. Question the employee's coworkers about any recent activity at the copy machine or taking a lot of work home prior to his or her termination.

- Conduct exit interviews with all employees. Remind employees of their continuing obligation to protect the company's proprietary information and that failure to do so could result in criminal and civil prosecution.

- Limit access to trade secret information to only those employees who have a need to know. Some companies, especially software houses, use a concept known as compartmentalization where engineers are only allowed to work on a piece of a project. In the majority of cases, the intellectual property taken was something the employee was authorized to use.

- Train employees and supervisors about the value of proprietary information, about their responsibility to protect it, and about how other companies or foreign intelligence agencies will try to obtain information. The close relationship scientists maintain with the academic community fosters an attitude that discoveries and certain information should be shared. Consistently remind employees that trade secret information is the property of the company.

- Institute a policy that requires management review of any speech or technical paper prior to its publication to ensure that confidential information is not inadvertently included. Most intelligence gathering is done legally, although often deviously, by reviewing trade journals, setting up sham requests for bid proposals, or eavesdropping on conversations at the local restaurant.

- Establish good telecommunication and data security procedures and controls. Protect desktop and laptop computers from theft. The value of the information on the hard drive is often more value than the hardware. Audit the security of your data maintained at offsite storage facilities. Maintain good network firewalls and monitor for large outgoing e-mail messages.

- One man's trash is another man's treasure. Create procedures for the collection and destruction of documents, tapes, QA rejects, etc. Every photocopier should have a paper shredder attached. Recycling companies that specialize in document destruction (be sure the dumpster is locked), and garbage compactors are also used to prevent the loss of information through the trash.

- Restrict the use of cameras by employees or visitors inside the facility.

- Improve document controls. Mark documents as confidential and include a warning that disclosure is a crime. Don't, however, mark documents unless they really contain trade secrets. This can dilute the legal integrity of your protections. Depending on the extent of your program, permit copying of documents by a sole copy room employee. Establish a secure library and require scientists to check their laboratory notebooks and other documents in and out. Initiate an authorization and sign out procedure if employees need to take sensitive documents home.

- Consider 'debugging' boardrooms prior to sensitive meetings. Although very few electronic eavesdropping devices are found, the value of the information discussed may justify the cost of a search. Be sure to secure the room after the search is completed and don't forget to close the drapes after the meeting begins.

- Strictly enforce all policies and procedures related to trade secret protection. A program without enforcement is worse than no program at all. It is possible to implement protective measures in the scientific community without sounding draconian.

If you are a victim of trade secret theft, consider the following actions:

- Do not confront or talk with the suspect. This will give them the opportunity to hide or destroy evidence.

- Contact the District Attorney or Federal officials immediately. Some companies either do not notify law enforcement or wait too long to do so. Even if the loss involves a patent dispute, it is important to obtain a search warrant to recover stolen property and to prevent its misuse. Companies often don't realize the magnitude of the theft until this step is executed. If you seek a search warrant, be prepared to follow through with criminal prosecution. Methods exist to protect your secrets from disclosure during a court proceeding.

- Maintain and safeguard evidence. Evidence may consist of such things as lab notebooks, computer transaction logs, and financial records.

- Consider a restraining order to restrict use of the information until the matter is resolved in criminal or civil court. Discuss these actions with your Corporate Attorney.

In spite of Benjamin Franklin's belief that "Three may keep a secret, if two of them are dead," good security procedures, employee awareness, and document control will help to keep sensitive information where it belongs. One trade secret can be more valuable than an employee walking out your door with a suitcase full of cash.