TheIntelligenceGroup®
RESEARCH ▾ INVESTIGATIONS ▾ FORENSICS

To Catch a Thief

When you suspect an employee of intellectual asset theft, it may already be too late.

By: Dennis P. Farley
Contributing Editor

Geoffrey Minx, the rising young star and top sales executive with Pharma Software, Inc., wrapped up a long day at the office by polishing off a few last emails and calling it a night. He packed up his laptop, loaded some papers into his briefcase and nodded to the security guard at the front desk on his way out. The proximity card reader picked up his ID at the door as well as the asset tag on his laptop, made the match between user and equipment and authorized his exit. Neither the proximity reader nor the security cameras detected the compact discs in his coat pocket, or for that matter the PDA in his briefcase.

Minx resigned his position with Pharma the very next day, reportedly to "pursue other business opportunities." He turned in his laptop and other equipment, surrendered his access card and had his remote access rights terminated. Within one week, Minx had started a competing business with a backlog of new sales—many of them former Pharma customers. His engineers were hard at work making modifications to Pharma's source code, and within the month would have a saleable, rival product on the market. In short, Pharma had been cleaned out.

After getting little interest from the local police, Pharma's security director led an investigation into the events preceding Minx's departure. The IT Department looked over Minx's former laptop and found no evidence of foul play. Employees recalled nothing suspicious. Pharma filed a civil claim with the court, which was ultimately tossed for lack of evidence. Geoffrey Minx was in business utilizing Pharma's assets, and nothing could be done to stop it. While the aforementioned persons and entities are fictitious, they highlight one of the greatest security challenges facing practitioners today—the securing of intellectual assets. Due to portability and ease of transfer, traditional security measures such as guards, cameras and access controls do little to mitigate the insider threat. In the preceding scenario, the Pharma assets stolen by Minx could have left the premises at least five different ways: email, laptop, paper documents, magnetic media (CDs) or his PDA. You couldn't get a cafeteria chair past the security guard, but no such protection was afforded the company's most valuable assets. Unfortunately, this is true of most organizations operating today.

Can You Stop It?

Stopping the Geoffrey Minx's of the world is not an easy task, as most often you have no idea it's coming. And, if you do suspect a high level executive of such theft, you're already somewhat late in the ballgame if you want to give yourself the best shot at stopping him in his tracks. However, there are a number of areas that organizations should consider, at a minimum, in order to prevent, and possibly detect, such behavior:

Adequately Assess Risk:

- Fact—approximately three quarters of computer-related security incidents occur from inside the organization.

- Fact—the pharmaceutical industry remains one of the most sophisticated markets for the practice of competitive intelligence.
  Minx's former company needed to understand they were vulnerable to different risks than other types of businesses. In their case, significant resources were allocated to keeping keeping outsiders out — physical access controls such as guards, card access systems and firewalls on the IT system—but little was put into

Integrate the Physical and Information Security Programs:

In Minx's case, the new source code that Pharma's R & D group was working on could have been accessed by Minx in a number of ways—none of which were given serious consideration by the security team. Perhaps access controls on the IT system were not adequate to keep this information secure only to the R&D users, and was easily accessed by Minx. More likely, internal physical access controls were not in place (software and tech companies often like open, collegial environments that foster collaboration), allowing Minx to forage the R & D area after hours. Perhaps he simply entered the data center via the propped open door (common) and accessed an unattended server with an open administrative session (more common). Or, perhaps he simply "socially engineered"an R & D colleague to get the latest line on products for anxious customers. Many organizations have two security related functions: the security director (guards, cameras, access controls, etc.) and an information security manager (principally firewalls, virus controls, access controls, etc.). Often, these functions aren't well integrated—sometimes they don't even speak regularly—despite the need to be good at both in order to protect the organization's most valuable assets.

Educate and Train Employees: While employee compliance is the weak link in most security programs, it goes much further. Most organizations do not understand the importance that employee awareness can play in securing assets. Training of the employees, especially in critical areas like R & D, can alert them to common aberrant behaviors that pose risk to security. Information security basics such as "need to know" and "social engineering" can alert them to internal threats like those actions exhibited by Mr. Minx.

Design for Later Investigation: Since most organizations don't discover the loss of intellectual assets until after the fact, you need to implement security systems that are designed to facilitate later investigation. And, you need to have a plan in place to adequately conduct intellectual asset investigations. Internal closed-circuit television (CCTV) backups and card access logs need to be maintained for a sufficient period. IT system access logs and audit trails need to be recorded and similarly maintained- so you can locate the employee at a time and place both physically and on the IT network. Appropriate computer forensic techniques need to be applied to adequately investigate equipment such as laptops, desktops and servers. The proper application of such tools can provide you with evidentiary documents that were deleted, which untrained IT staff cannot even see on the computer. In Minx's case, the Pharma IT staff saw nothing, despite the deleted download of R & D source code as well as a variety of emails with colleagues indicative of early collaboration. Each of these documents could have been made available to the court if properly secured with forensic techniques. Response capability by professional computer forensics experts needs to be part of every security plan, as it's not traditionally a job for the IT staff.

You Have the Right to Monitor: According to the American Management Association, 82 percent of American business used some form of electronic monitoring in the past year to track their employee's habits. This includes not only security cameras and card access systems which monitor their movement, but Internet and e-mail monitoring systems that can track the flow of information. Such software can be set up on the organization's mail server, simply filtering outbound and inbound traffic for key phrases—such as source code indicative of the organization's most valuable asset. When detected, these emails can be blocked and quarantined for subsequent review by a member of the security staff. The key to making such monitoring tools useful and effective is appropriate policy— employees need to understand, and acknowledge, that they have limited expectation of privacy within the workplace.

a member of the security staff. The key to making such monitoring tools useful and effective is appropriate policy—employees need to understand, and acknowledge, that they have limited expectation of privacy within the workplace.

What If I Suspect Somebody Today?

If you do suspect an individual of intellectual asset theft, there are some steps you can take to satisfy your suspicion—assuming you already have the right policies and procedures in place. Electronic data stored even temporarily leaves a fingerprint, and most systems make a record of how they were accessed. In such situations, it is not uncommon to covertly investigate the suspect for signs of aberrant behavior. A covert, forensic evaluation of an unsuspecting subject's computer, for example, can reveal information that was accessed, emails and other documents providing evidence of plans, etc., and Internet histories. Reviews of access logs and audit trails can reveal evidence of information downloads from the IT system. Reviews of physical access logs, CCTV records, etc., can reveal odd hours or visits to physical locations within a facility that are suspicious. The key is to gather this information in a covert fashion, as an organization's credibility is at stake when, and if, accusations of such behavior are made. In the world of intellectual asset security, there is no "magic bullet." No one, simple, elegant solution exists, simply because of the fact that access must be granted to insiders such as employees in order to do their job. Keeping your assets secure, therefore, is dependent on effective monitoring and detection programs that allow you to act quickly when loss is suspected, and provide solid evidence for prosecution when it does occur. ?

About the Author
Dennis P. Farley *is president of The Intelligence Group, a national investigations firm specializing in electronic intelligence and information security. He can be reached via email at* DFarley@intell-group.com

Reprinted from Security Magazine