Auditing Your Disaster Recovery Plan:
A Closer Look At High Tech Crime Will This Be Your Most Likely Disaster in the 21st Century?

By Jack Wiles, Director of Oltronics, Inc.

Everything is high-tech these days including the minds of the world's criminal element. If they find an opportunity, they won't think twice before breaking into your corporate computers and possibly causing you the biggest 'front page news' disaster that you could ever imagine. It has already happened to a number of organizations . Do you have the necessary controls in place to prevent this type of disaster? As an auditor, you will be the one responsible for the investigation, evaluation and verification of any controls in place which could help reduce the Risks associated with this new type of disaster. New Threats are making headlines almost daily. Technical and physical Countermeasures are being made available just about as quickly.

Your corporate Disaster Recovery Plan is a very valuable document. It needs to be audited as closely as any other important company asset. I'd like for you to consider these new threats of High-Tech Crimes such as Information Warfare, Industrial Espionage, Denial-Of-Service Attacks and variety of White Collar Crimes that continue to make headlines. Does your Disaster Recovery Plan address any of these new threats?

Disaster Avoidance
This is always better than Disaster Recovery. Putting together a good plan, and auditing it regularly can go a long way towards preventing a disaster. Most disasters involving High-Tech Crimes can be prevented! That's where you come in. Being the eyes and ears of senior management places you in an interesting position. When you make a suggestion as to how to protect the organization from a possible disaster, your suggestion will be heard by the right people. They may not react to the suggestion, but at least you've made them aware of it.

A Closer Look At High-Tech Crime
Crime has been with us throughout recorded history and undoubtedly longer than that. Our law enforcement and criminal justice systems have centuries of experience in dealing with all of the issues associated with most crimes. HIGH-TECH Crimes are the new kid on the block, and they are just a little bit different than the crimes that we have all been used to. We need to take a closer look at this growing threat as we rapidly head into the 21st century. This is truly an area where disaster avoidance and prevention are many times more valuable than recovery after an incident.

Undetected
The news is now full of stories associated with this new type of HIGH-TECH Crime. I read an article last year which stated that 97% of all HIGH-TECH Crimes go UNDETECTED! That's undetected, not unreported. That would be like someone breaking into 100 houses in your neighborhood and having 97 of the owners not even become aware that they had been victims of the break-ins. Have you been a victim of one of those 97% undetected HIGH-TECH Crimes?

Proactive, continuous checking will be our only hope as we head into a 21st Century that will be more HIGH-TECH than we can even imagine. Everything that matters in our lives and on our jobs will be closely related to computers. We need to stay aware of what those computers are being used for and who has access to the valuable information residing on them. The HIGH-TECH criminals of the world are counting on the fact that most people don't keep a close watch on their computers. They want that 97% undetected crime rate to go to 100%. Only you can help the percentage to go the other way!

What Are The Crimes?
Unfortunately, computers are susceptible to more types of crime than just about anything else in your home or office. Not only do they face the old standby crimes of physical theft, destruction and vandalism, the newer more HIGH-TECH crimes may be even more damaging to you as the computer owner.

Any Risk Assessment performed today will probably reveal that your most valuable asset is residing somewhere on a hard drive rather than in a company safe. The "bad-guys" of the world are well aware of this newfound safe waiting to be cracked. I have seen the statement made in several articles that criminals can now do much more damage with a keyboard than with a gun. The actual crimes include software piracy, stealing source code, stealing credit card numbers, stealing passwords and login ID's, industrial espionage, stealing customer account information, stealing employee personal information, PBX fraud, intentional insider damage and many others.

Federal and State computer crime laws need to be looked at frequently as new laws are added or current laws are changed. There were no laws that applied to computer crimes until about 8 years ago. Now there are many, and there will probably be more added as things get worse.

Crimes At Universities
Colleges and universities are not immune to high-tech or any other type of crime. I use a number of war stories in my seminars to help others learn from them. The one that I most remember when I think about colleges and universities is a crime that involved grade fixing. As with most 'war stories', the names of the criminals and victims as well as the location of the crimes is unimportant. The fact that this happened to someone at some college or university means that it could happen to you.

The newspaper articles that covered the story didn't say how long this crime had been going on. They did cover the arrest and later conviction of the person involved in the grade fixing. For a while, all grades of current and former students were in question. Did the students really earn them, or did they pay someone to 'fix' them in the database. Needless to say, this wasn't a comfortable situation for the students or the school. Any headlines of this nature hurt everyone involved.

How Easy Was It?
Crimes involving computers and people are frequently too easy to commit and too difficult to track. Unless there is something else involved to really establish guilt, simply looking at audit trails and database records may not 'prove' who actually committed the crime. It may be too easy for someone to look over your shoulder as you type in your logon I.D. and password. If there is no other form of authentication being used, whoever looked over your shoulder could type the same thing and the computer would let them in as easily as it let you in. Does it know who typed the logon I.D. and password? Computers aren't quite that smart yet! If someone gets your password and uses it, all audit trails will show that 'you' did whatever is done during that unauthorized session.

There are fairly inexpensive ways to provide authentication (and protection) for all users. Dynamic password generators have been on the market for about ten years now, and their usage is becoming a standard of care in many industries. It would be worth your while to look into them.

Who Are The Criminals?
This is another question with a moving answer. We used to blame this problem on what the media frequently called "hackers". I have always preferred the term "crackers" for those who actually break into computers, but these are far from the only threat. Just about every other type of criminal out there has now figured out that what you have sitting on that hard drive (frequently wide open for the taking) is an easy mark. You need to ask yourself "If all of the information on my computer were printed out on paper, who would like to have a copy?" Who would like to sell it to your competitors? Who would like to destroy it so that you wouldn't even have access to it? Would any of your employees be disgruntled enough to get involved with criminals? When was the last time that you took an inventory to see exactly what you do have on those hard drives? Has an employee put something there that could really hurt you?

If there is one thing that has totally shocked me over the years as I have worked with law enforcement on some of these issues has been the types of people who became HIGH-TECH Criminals. Some are professionals with advanced degrees from some of the best schools in the Country. Hopefully, one of them in not sitting in your office today.

War Stories And Lessons Learned
War Stories are simply lessons learned at the expense of someone else. I share a number of them in my seminars, and they are quite effective in helping to prevent similar problems from happening to those attending the seminar. Here is one of my most helpful War Stories:

Everything was going well for the owner of a very successful company. Her company had grown, and her computer network had grown with it. Things were going so well that she established a broad band (T-1) access to the Internet for the purpose of doing more business. One of her employees had been with her for some time and had been given the responsibility of being the System Administrator of the computer network in this ever growing company. Things were going well.

As the computer system grew, more disk storage was needed, and the System Administrator did a great job in keeping up with the growth. Gigabyte size disk drives were getting cheaper, and several new ones were added to the system to allow for growth. Her System Administrator devoted as much time as was necessary in keeping up with the technical growth. This meant many long nights and weekends for this dedicated person. Those of us who work in the technical world know all about those long nights and weekends. Things were going well.

On a Monday morning not long ago, things Stopped going well! Her very dependable system administrator who never missed a days work, didn't show up for work at all. Several hours passed, and my friend was getting concerned about the whereabouts of this person. She didn't have to wait much longer. At about ten that morning, a Federal Agent was handing her a Search Warrant. This would be a little more than a typical Monday.

Is seems that her trusted System Administrator had been arrested and charged with being a part of an international pornography ring. My friends computers and T-1 access to the Internet were being used to house and distribute these pictures to the rest of the ring. Now it was becoming more clear why those extra gigabyte drives were installed, and why the T-1 access was so highly recommended by this person. It takes a lot of disk space to store digitized pictures, and a lot of bandwidth (T-1) to quickly transfer or print them. Now all of those long nights and weekends made a little more sense.

Needless to say, my friends life will never be the same. She has had to get an attorney to represent her as well. After all, it was her computers and her Internet address that all of this was happening on. Once a crime has been committed, everything involved needs to be looked at closely. She has learned from much from this very uncomfortable incident. She will never hire anyone again without having a per-employment screen performed. She will not allow any single person to be the only one who knows everything about her technical network. She will have occasional integrity checks performed by outside consultants. She will take a much more active role in knowing exactly what is on her corporate computers. Hopefully, you can learn a little from her experiences and prevent something like this from happening to you.

Seized Evidence
These new ‘high-tech’ crimes may cause companies even more problems after they have been victimized. What if your corporate computers become ‘seized evidence’ because of something that was committed from inside your company? For a small to mid-size company, this could be devastating. Might your backup tapes also be involved? Do you know what’s on them?

Our experiences so far in this ever changing world of ‘high-tech crime’ have taught us a valuable lesson. The time spent PREVENTING your disaster will be much more wisely spent that the time spent trying to recover from it. As technology speeds towards giga-bytes of memory and tera-byte size disk drives sitting on desk tops, this problem will only get worse. Start preventing your disaster today!

Where To Go For Help
Since the laws that address HIGH-TECH Crime are so new, most people that I meet don't know who to call for which type of crime. A good rule of thumb that I use in every situation is to call your local law enforcement agency first. They know you and your neighborhood better than anyone else. Many are now trained to respond to these new types of crimes. They will also know more about which state or federal agency to call for your particular situation.

If you do call a state or federal agency first, at least let your local agency know about your situation as well as the fact that a another agency is working on the case. What you don't want is to have two agencies working on the same case and not knowing it. Our law enforcement resources are always overworked, and we don't want to waste any of their time.

Several federal agencies are very involved with HIGH-TECH Crime. Among these are the Secret Service, the FBI and U.S. Customs Service. Each investigates different types of crime, and certain crimes are worked on by more than one agency. If in doubt, pick one and call them. They will head you in the right direction.

THE HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION (HTCIA)

There has been an association formed to help assist with these types of crimes. They are called the High Technology Crime Investigation Association (HTCIA). The first chapter of this association was formed in the Silicon Valley area in California about ten years ago. There are now about 12 chapters throughout the country, and several are being formed in other countries which will make it an International Association.

The HTCIA chapters throughout the country offer some of the best training available for both law enforcement agencies and corporate security specialists. Many of my associates in Contingency Planning and Disaster Recovery positions are also members of an HTCIA chapter. For additional information concerning activities and membership you can contact me directly. I am currently the President of the Carolina Chapter.

Some Excellent Security Related Books
There are several books available which specifically address computer and network security. This list will undoubtedly grow as the headlines create more awareness of this topic. There are two books that I highly recommend to everyone concerned with these issues. Both of them address only one topic, Computer Crime! Just because they were written to describe this single topic doesn't mean that they are casual books. One is almost 450 pages in length, and the other one is over 600 pages. In my opinion, you need to consider both of them.

The first one is titled "Computer Crime, A Crime Fighters Handbook". It was published by O'Reilly & Associates and written by David Icove, Karl Seger & William VonStorch. It provides an excellent overview of the topics and issues associated with preventing , investigating and prosecuting these new high-tech crimes. The ISBN number is 1-56592-086-4 and my copy was $24.95 which I believe is the retail price.

The second book is titled "High-Technology Crime, Investigating Cases Involving Computers". This is an in-the-trenches nuts and bolts book over 600 pages in length. It was written (it took four years to write) by Mr. Ken Rosenblatt who is a Deputy District Attorney for Santa Clara County, California. For those of you who haven't been there, that's "Silicon Valley".

Mr. Rosenblatt packs a lot of front line experiences into his book. He should know, he headed the offices High Technology Crime Unit for four years and is a graduate of Stanford Law School. I went into a little more detail about him for a reason. When people with this kind of background take the time to put their years of experience into writing, we all need to know that the finished work exists.

This book is extremely well written, and it will save law enforcement investigators, corporate investigators, prosecutors and corporate counsel hundreds of hours by providing proven step-by-step procedures for investigating cases involving computers. There are nine detailed check lists provided as well as example search warrants. There is even a 3 ½" diskette included with the book which contains the checklists and search warrants in text form for you to bring into your word processor.

You won't find this book in bookstores. It must be ordered directly from the publisher. In my professional opinion, if you have a need to know more about this world of High-Tech Crime, you could not invest your money more wisely. Here's where to order it or to write requesting more information:

KSK Publications, P.O. Box 934, San Jose, CA 95108-0934

Prevent Your Disaster Now - Later May Be To Late
Having been involved with security for over twenty-five years, I now have enough "War Stories" to last another life time. There are two words that I dread hearing as someone approaches me with another real life disaster story. Those words are "IF ONLY"! If only I had listened and spent more time preventing this from happening. We are all very busy, and it doesn't appear that things will slow down any time soon. Security,

Disaster Avoidance and High-Tech Crime prevention are issues that will occupy your time sooner or later. Why not make it sooner so that you won't ever have to say "IF ONLY"!

Sleep Well

About the author:
Mr. Wiles is Director of Oltronics, Inc. Security Services Division. He is also President of the Carolina Chapter of the High Technology Crime Investigation Association (HTCIA) and a member of the Contingency Planning Association of The Carolinas (CPAC) . He can be reached on (803) 328-2753 or at jwiles@oltronics.net *on the Internet.*