Case Study of Insider Sabotage: The Tim Lloyd/Omega Case

By Sharon Gaudin

The government has just sent a message to every would-be hacker or corporate computer saboteur: you can be caught and put away.

That's the word coming down after the May, 2000 conviction of a former corporate network administrator in the first federal prosecution of computer sabotage.

"This tells everyone that we're capable," says Assistant U.S. Attorney V. Grady O'Malley, who prosecuted the case for four weeks in Newark District Court. "There are people out there who believe they can't be caught. They think [the general public] isn't as smart as they are, and if they are, they're not in the government… This shows them that we can track down the evidence, understand it and logically present it to a jury."

O'Malley, working in conjunction with Special Agents of the United States Secret Service, won the conviction against Tim Lloyd, 37, of Wilmington, Delaware. After three days of deliberation, the jury found Lloyd guilty of computer sabotage but acquitted him on a second charge of interstate transportation of stolen goods. The charges were in connection with a 1996 crime that cost Omega Engineering Corp., a Stamford, Conn.-based high-tech measurement and instrumentation manufacturer, more than $10 million, derailed its corporate growth strategy and eventually led to the layoff of 80 workers.

The government laid out a story that spanned 11 years. It was the story of a trusted employee who rose through the ranks of a relatively small company to the point where he ultimately planned out and built Omega's first computer network for its Bridgeport, N.J.-based manufacturing plant—the heart of this manufacturing company. But as the company expanded into a global enterprise, Lloyd's prominent position slipped into that of a team player. Feeling 'disrespected', Lloyd turned on the company, planting a software time bomb that destroyed the hub of the network that he himself created.

And that one move destroyed more than a thousand programs that ran the company's manufacturing machines. It also brought a global enterprise, one that supplies instrumentation to NASA and the U.S. Navy, to its knees. All in the matter of a few seconds.

Today, Omega still is struggling to right itself and reclaim its position in the market. And Lloyd, who maintains his innocence, awaits sentencing, which is slated for July 31, four years to the day after Omega's file server crashed. He faces up to five years in federal prison. Omega faces an untold number of years trying to rebuild.

"We will never recover," Jim Ferguson, plant manager at Omega South, Omega's Bridgeport manufacturing plant, told the jury.

Industry analysts note that the high-tech community has long scoffed at government efforts to keep track of them or even to keep up with them.

That gap in knowledge and skill seems to be growing shorter.

Ken VanWyk, corporate vice president and chief technology officer of Alexandria, Virginia-based ParaProtect, a computer security portal, said this case will have historical and legal significance, setting a precedent for how computer security crimes are handled.

"You're looking at a lot of damage here," said VanWyk. "The company has been greatly damaged. How easy is it to track down digital evidence? How easy is it to find the culprit following a digital trail? How easy is it to make a jury understand the technology? These are all questions that are being answered."

And O'Malley said the answer has come in loud and clear.

"These people should realize they are no longer invulnerable," he added. "This type of crime is no longer a mystery and there is some bite to computer crime statutes."

Bomb cripples manufacturing

It was the morning of July 31, 1996. The first worker in the door of the CNC (Computer Numeric Control) department at Omega South fired up the Novell NetWare 3.12 file server just as he always did. But this time, the server didn't boot up. Instead, a message popped up on the screen saying that a section of the file server was being fixed. Then it crashed.

But it didn't just crash. When the server went down, it took nearly every program down along with it, destroying any means of finding them and scattering the millions of lines of coding like a handful of sand thrown onto a beach.

Omega executives didn't know this yet, though. All they knew was that the server was down and the manufacturing machines were sitting idle, waiting for the tooling programs that had been stored on the file server.

Ferguson, who had immediately been called when the server crashed and failed to reboot, said he went looking for the backup tape while other workers tried to bring the server back up. Even if the server was down, the programs could be taken off the backup tape and the machines could run.

Ferguson, who had immediately been called when the server crashed and failed to reboot, said he went looking for the backup tape while other workers tried to bring the server back up. Even if the server was down, the programs could be taken off the backup tape and the machines could run. The backup tape was nowhere to be found, however.

Ferguson, as he testified in court, then went to the individual workstations to retrieve any programs that workers had saved to their desktops. There was nothing for him to find there either.

"It was an awful feeling," Ferguson says.

With no programs and no backup tapes, Ferguson says he had few options but to order the machines to run with the programs that already had been loaded on them the day before. He had to keep his people working, his machines pumping out products. And the machines did run like that—some for days, some for weeks. They ran like that until they choked inventory or exhausted their raw materials.

"We were doing everything we could. The other step would have been to shut down and lay off everybody," Ferguson told the jury. "We were just starting to get an idea of all the impact and what this was going to mean and how it was going to affect us."

It was only a matter of days before three different people called in to do data recovery all reported that the programs were nowhere to be found.

And that was the beginning of an IT nightmare that still haunts Omega to this day, according to several executives who testified in the trial.

Ralph Michel, Omega's chief financial officer, testified that the software bomb destroyed all the programs and code generators that allowed the company to manufacture 25,000 different products and to customize those basic products into as many as 500,000 different designs.

"That department gave us flexibility to modify our products and gave us the ability to lower our costs," said Michel, who noted that Omega had shown 34 years of growth but started slipping after the computers crashed. "We lost both of those advantages in July 1996. . . I believe the server crash was one of the principal reasons for the drop in sales, if not the reason."

Michel noted that Omega's sales efforts took such a hit because of the company's inability to manufacture products without a long lead time that within two years after the crash, Omega was showing a 9% drop, which equals about a $10 million loss. And Michel added that Omega had shown only increases in annual sales since 1962.

Tracking down the cause of the crash

And while the company suffered financial and market hits, Ferguson and other plant managers looked to retrieve the programs and get manufacturing on its feet again.

And immediately, their attention turned to their former network administrator—Tim Lloyd, who had been

What happened to Omega Engineering, Inc. could happen anywhere

Here are a list of ways to protect your system:

- Make sure no one person is controlling the system front to back;
- Every logon should have a password;
- As few people as possible should have supervisory rights;
- Mission critical systems should be backed up every day, and every system should be backed up weekly;
- Have a strict sign-in/sign-out system for backup tapes;
- Always have a current copy of the backup tape stored remotely;
- Do backups of desktops and laptops, as well as servers;
- Rotate backup tapes – don't keep using the same one over and over again;
- Change passwords every three months;
- Keep servers in a secured area;
- Stay up-to-date on software patches;
- Use intrusion detection software that alerts you when you are being hit and make sure your response time is faster than a fast penetration;
- Code should not be put up unless at least two pairs of eyes have checked it over;
- Have an information security department (at least one person and then one other for every 1,000 users) that is separate from the IT department and reports directly to the CIO;
- At least 3% to 5% of the IS budget should be spent on information security;
- Information security personnel should be aware of any employee who is showing signs of being troubled or disgruntled, particularly if that employee holds an information-critical position;
- Beef up security during certain events, such as mergers or downsizings, that could upset workers and cause them to lash out at the company;
- If an employee, particularly an IS employee, is becoming a problem, start locking down—monitor the network, set up software that will alert you if she is in a different part of the net work than unusual or if she's working at a different time than usual. Also, scan email to see what's going out of the company, double check backup tapes and have someone else do the backups if that person is the one in question

fired three weeks before the crash.

Lloyd, who had started out at Omega in 1985 as a machinist, had worked his way up the line until he was the sole person in charge of the network—the network he created. Lloyd handed out passwords, maintained the server, loaded new programs and worked on any expansions. He also was in charge of doing backups and, as Ferguson later discovered, had recently taken programs off the workstations and centralized them on the one file server, telling workers not to store them locally any longer.

"I had trusted Tim Lloyd completely," Ferguson told the jury. "We relied on Tim Lloyd… I trusted Tim to maintain the backup tape. He was responsible for the security of the system."

And Lloyd had taken out the backup tape on July 1. Now, weeks later, with the system down, the tape was nowhere to be found.

"Tim, Tim do you have the backup tapes?" says O'Malley describing Ferguson's desperate call to Lloyd after the crash. "Tim, we need those tapes. Are you sure you don't have the tapes?"

The Code and How it Works

1. 7/30/96
   n The date is the triggering point in the code string, executing the rest of the commands as long as it is after July 30, 1996.

2. F:
   n This line of the code gives access to the server.

3. F:\LOGIN\LOGIN 12345
   n This automatically piggybacks User 12345, which has supervisory rights and no password security, with whichever user first logs in on the file server.

4. CD \PUBLIC
   n This line gives access to the public directory, a common storage area on the file server.

5. FIX.EXE /Y F:*.*
   n FIX.EXE is a DOS-based executable that served as the deletion command but showed the word 'fixing' on the screen instead of 'deleting.' This is a slightly modified version of Microsoft DOS' Deltree.exe.
   n /Y answers 'yes' to the implied question of 'Do you want to delete these files?'
   n F:*.* refers to all files and folders on the entire server volume

6. PURGE F:\ /ALL
   n This line calls for all of the deleted information to be immediately purged.

Ferguson says Lloyd told him he didn't have the backup tape. Lloyd, according to testimony, says he left them in the upper left-hand corner drawer of his desk at Omega. But Ferguson himself had helped clean out Lloyd's desk. There was no backup tape there.

Ferguson called Lloyd again and again. Once, Lloyd said he would check around his house but never called back. Ferguson called again and Lloyd said he hadn't had a chance to check. Ferguson called again and Lloyd told him he had some tapes but not Omega's tapes. Ferguson then recorded one of his calls and went to Lloyd's house to plead in person. While he was there, Lloyd handed over a pneumatic pump, a computer case and a power cord. No backup tape.

The plant manager says even while he was pleading with Lloyd for information about the tape, he still was having a hard time imaging that Lloyd would have damaged the system. Ferguson had held on to that kind of trust even when Lloyd had become a problem employee.

About a year earlier, Lloyd went from being a star employee to an angry man who lashed out, verbally and physically, at his co-workers, bottlenecked projects simply because he wasn't in charge of them, and even knowingly loaded fault programs to make co-workers look bad, according to Omega executives. In that year, he had received verbal warnings, was written up twice and demoted.

Lloyd was lashing out at his co-workers, as O'Malley

told the jury, because his ego was bruised. He was the genesis of the network and suddenly his status and clout were slipping away from him. And a team player he did not want to be.

The prosecution contends that Lloyd, who had started interviewing for a new job early in June of 1996, had started planning to leave Omega months before he was fired. Either way he was going out the door, he was planning on leaving a parting gift for the company that had "disrespected" him, according to O'Malley.

On July 10, 1996, Lloyd was fired. "The day I fired Tim Lloyd wasn't a happy day," says Ferguson. "Here was an individual I worked with for 11 years. I was very frustrated with how things worked out toward the end."

And during all of this, no one at Omega assigned someone other than Lloyd to do the backups. No one checked the file server before or after he left. No one even hired a new network administrator after Lloyd was terminated, assuming that all it needed was simple maintenance and an outside contractor could take care of that. The comapny was running on trust.

> The plant manager says even while he was pleading with Lloyd for information about the tape, he still was having a hard time imaging that Lloyd would have damaged the system. Ferguson had held on to that kind of trust even when Lloyd had become a problem employee.

The Secret Service takes over the investigation

On Aug. 12, 1996, Omega executives called in the U.S. Secret Service, which splits its time between protective service and conducting financial and high-tech fraud-related criminal investigations. The Secret Service is one of the government's biggest weapons against computer crime. A relatively new statute makes computer sabotage a federal offense if it affects a computer used in interstate commerce and causes more than $5,000 worth of damage to the company in a 12-month span of time.

On Aug. 14, Special Agent William D. Hoffman arrived at Omega and began an investigation that would span the next four years. Hoffman, who has been with the agency for four years, began by interviewing about 50 Omega employees, everyone from company owners to people working the lathe machines on the shop floor.

"It was apparent to me very early on that this was not an accident," says Hoffman. "The files that had been deleted were surgically removed from the database. They specifically were the files the company needed to survive."

And early on, the evidence pointed directly at Lloyd. Hoffman pointed out that Lloyd had Novell certification training; he had complete access to the system, and he was the last one with the backup tape.

Hoffman also notes that they checked out Ray Nab, another former Omega employee. Nab, who was a friend of Lloyd's, had been a CNC programmer and had quit the day the file server crashed. Nab, however, took and passed a lie detector test. And Hoffman says Secret Service agents searched Nab's house and didn't find anything connected to the crash or to Omega.

Hoffman, along with several other Secret Service agents, conducted a search warrant on Lloyd's home Aug. 21, 1996. The agents seized about 700 pieces of potential evidence. That haul included computers, motherboards, keyboards, more than 500 disks, CD-ROMs, 12 hard drives and tapes.

"It was enormous," says Hoffman.

What immediately stuck out from that haul were two backup tapes, which had both been erased. One was labeled Backup with the dates 5/14/96 and 7/1/96 and the words Tim Lloyd. July 1, 1996 was the date that Lloyd had asked for and been given Omega's backup tape. Both had been reformatted, which erases the tapes, the day before Ferguson visited Lloyd's house asking about the tapes.

"The moment I found out the backup tapes had been reformatted, my level of suspicion was elevated dramatically," says Hoffman.

Tracking down the destructive code

While Hoffman was tracking down physical evidence, technicians at Ontrack Data International Inc., a data recovery firm out of Eden Prairie, Minnesota, were searching what basically was a digital debris field on a

mirror image of the damaged file server. Omega had called in Ontrack about a week after the server crashed to try to recover the missing programs.

Months into the effort, Ontrack conceded that the programs simply were not recoverable. Then they turned the copy of the server over to Greg Olson, director of Ontrack's Worldwide Data Recovery Services. Olson was focused on finding out what caused the crash.

"We do data recoveries when companies are losing millions of dollars a day," says Olson, who has written data recovery tools for the NetWare operating system and even was brought in by the U.S. government to recover files off of some of Kuwait's computers damaged during the Gulf War. "It's not uncommon for me to be working with people in panic mode but… I've never seen this massive of a deletion in my 10 years of experience."

Olson says there were several things that raised red flags for him right from the start.

"It was odd that the user accounts, most of them, had supervisory rights," he explains. "It's odd that Account 12345 had supervisory rights and no password… Our system administrators would freak out if they knew there were half a dozen accounts with supervisory access… It violated the principles of security."

With these red flags in the back of his mind, Olson started out doing searches for common commands or phrases used in deletions, such as DEL /S; *.*, DEL F:, DELTREE F: and PURGE F:\.

"I was just thinking of common things to search for and these were taking hits," says Olson. "Immediately, I knew this was hot when I saw PURGE take a hit."

Olson continued to systematically pull programming strings, sitting in their raw form, out of the code wreckage until he had pieced together six lines—six lines that looked like they could do some real damage. "What's unusual are these six strings together," he says. "First of all, the date was meaningful because the data loss was the next day. The second thing was this login account 12345, which had supervisory rights and no password. We'll say that's not recommended. The next thing unusual is the fifth line that refers to all the data on the server and /Y is a common command line switch to make the program default to yes.

"This is the type of stuff you'd find in a utility to do mass something," Olson adds. "The last thing is the PURGE. Having the PURGE there with the F:\ refers to the server and everything on it. And combined with that date, it was very unusual. You're not going to go into another company's file server and find that combination of strings. That was definitely a red flag situation."

And from there, Olson set out to determine what part FIX.EXE, which is not a NetWare executable so would not normally be found on a NetWare system, played in the string. The way the strings were set up, he says he knew FIX.EXE must have deletion powers but now it was a matter of proving it.

> "It was apparent to me very early on that this was not an accident,'' says Hoffman. "The files that had been deleted were surgically removed from the database. They specifically were the files the company needed to survive.''

So Olson went out on the drive and pulled off 670 raw executables. He tested each and found one that appeared to be DELTREE.EXE, a DOS-based command that enables administrators to delete files off Windows operating systems.

"I pulled DELTREE and executed it with these command lines to see what would happen," says Olson. "I was shocked when the normal DELTREE function, saying 'deleting this, deleting this', was replaced with 'fixing this, fixing this'… I knew I was on to something there."

What he knew was that the DELTREE executable had been modified to disguise its deleting message by dropping in a 'fixing' message in its place. That was FIX.EXE. That one step camouflaged the deletion process so the user logging onto the system would never know what was actually happening.

Testing the six-line program

To test the code, Olson took an exact copy of the Omega file server and set up a test environment with an attached workstation. He then set out configuring the system for various dates prior to the July 30, 1996 date at the beginning of the code string.

Olson configured the system for Jan. 1, 1996 and logged in. Nothing unusual happened.

Then he configured the system for April 30, 1996 and logged in. Nothing unusual happened.

He then tried July 29, 1996. Nothing unusual happened.

Olson then tested July 30, 1996, matching the configuration date up with the date in the code. Nothing.

Then he configured the system for July 31, 1996, one day after the date in the code and the exact date of the crash at Omega. "I logged on and everything on the system was deleted," he told the jury. "On the screen, it was saying it was fixing an area of the system, but actually it was deleting everything… Everything was gone."

"The puzzle had been put together," he adds. "There's absolutely no doubt in my mind that this is what caused the data loss."

And Olson says some planning went into this. Along with the six lines of code that did the damage, Olson also found three similar test programs. Those three programs, each similar to the six lines of code in the damaging program, were dated Feb. 21, 1996, April 21, 1996 and May 30, 1996. The first two programs had only one line that was dissimilar from the damaging code. That one line substituted a simple test folder, which could have held as little as one word, for the line in the damaging code that called for everything on the server to be deleted. The third test program dated for May 30 was set up exactly as the code that brought down the system.

The government proves its case

"When Ontrack found the data string, I knew this was it," says Hoffman, who flew out to Minnesota to be at Ontrack for three days in February of 1997 while Olson figured out exactly what those six lines could do. "Before that, we had not proven the [federal] violation for sabotage. We didn't know what had caused this massive deletion. When he called us, we had intent."

With the code in hand, Olson went looking through the rest of the hard drives that Hoffman had given him to examine. And in that pile, he found those exact same six lines of code on one of Lloyd's personal hard drives that also stored his PR photos, his checkbook software and personal letters.

"That's when I knew we had our guy," Hoffman says.

Lloyd was indicted on Jan. 28, 1998. After several postponements, the trial started on April 17 of this year.

During the trial, Lloyd's attorneys told the jury that this is the case of a computer that simply crashed. They also said this is the case of Omega executives, who had been lax in their own jobs, casting aspersions on someone else to cover up their own failings. Defense contends that the crash could have been caused by an outside hacker, by another employee or by a virus.

> What he knew was that the DELTREE executable had been modified to disguise its deleting message by dropping in a 'fixing' message in its place. That was FIX.EXE. That one step camouflaged the deletion pro-cess so the user logging onto the system would never know what was actually happening.

Lloyd, who did not testify, said in an interview after the verdict came in that he is innocent of the crime.

"There's no way in the world I did this," says Lloyd. "I had complete access to the mainframe system from home… If I was a vindictive person, do you think I'd go after a teeny, tiny little network?"

But O'Malley told the jury it could not have been anyone other than Lloyd who could have taken that file server down in such a strategic and calculated fashion.

"Was the real guy sitting next to Tim Lloyd and fiddling with the system and changing dates?" O'Malley asked the jury. "I suggest not. Who could do all this and not be questioned by the administrator? No one. It was the administrator… He was setting this up months in advance."

Protecting a company from the predators inside

What most industry analysts point out is that while Lloyd may have spent months setting up his plan, it's

more time than the company put in to protecting itself from insider attacks. And that doesn't make Omega any different than what many say is a majority of companies out there.

Analysts generally agree that while companies are hot on buying firewalls and anti-virus software, they're extremely lax when it comes to looking at the potential risks that come from within. And most also agree that inside attacks are more of a problem than outside hackers—both more common and more potentially harmful.

Depending on the source, industry analysts say in-house security breaches account for anywhere from 70% to 90% of attacks on corporate computer networks. Analysts note, however, that number is probably skewed since they believe most insider attacks go undetected. Dennis Szerszen, director of security strategies at The Hurwitz Group in Framingham, Mass., says that for every in-house attack reported, there could be as many as 50 that go either unreported or undetected.

Screaming newspaper headlines and news reports about denial of service attacks or malicious teenage computer geniuses running rampant on the Internet have garnered most executives' attention—and their budgets.

That means if CIOs or CEOs aren't paying attention to the right risks, they're not spending their security budgets in the right place, either.

"I think a lot of companies will buy a firewall and think they have a security infrastructure in place," said Amit Yoran, president and CEO of Alexandria, Va.-based RipTech Inc., a $10 million security consulting and service company. "That's a big mistake. They also consider anti-virus software to be a security solution. Those are good things but they're not everything."

Most analysts say firewalls, anti-virus software and another hot security commodity, Virtual Private Networks—all of which are focused on securing the perimeter—are just part of a security strategy since they may only be addressing 10% to 30% of a company's security needs. Companies also need to look at technology that will protect their information from those who already are on the inside.

Companies need to remember that every employee, whether a programmer, head of marketing or the network administrator, could potentially pose a problem. And it's the people on the inside who know exactly where information is stored and what strikes will hurt the most.

Matthew Kovar, a senior analyst at The Yankee Group, says having too much faith gets many companies in trouble.

"They think they know everyone. They think they have trusted employees," says Kovar. "That philosophy breaks down sometimes—some would say quite often… The reality is that most people aren't deploying technologies to alert themselves (to inside breaches). They don't even know it's happening."

Sharon K. Gaudin *is a features writer for Network World. With four years of computer-related reporting under her belt, she covers a broad range of topics for the weekly publication, including network security and management, operating systems, wireless technologies and employee management issues. Before working at Network World, she covered Microsoft Corp., Novell, Inc., software development and the security beat for Computer World. And prior to that, she held an array of positions for mainstream newspapers, ranging from executive editor to business editor and online editor. Today, she lives and works on the Maine Coast.*