



*Excellence in
IT Security & Investigations*

CASE STUDY: INDUSTRIAL ESPIONAGE & LOSS OF TRADE SECRETS

INDUSTRY: RESEARCH INDUSTRY POTENTIAL LOSS: \$100 MILLION

CHALLENGE: INSIDER THREAT TIME TO RESOLVE: 7 DAYS

Background: The Chief Information Security Officer (CISO) of a research company was made aware of unusual activity by one of the company's employees. A researcher was observed running a piece of software that was a known hacker tool from his laptop computer on the company's research and development server. An action which the subject employee, who held a PhD in Computer Science and Mathematics, was not authorized to do. The CISO of the corporation immediately called in Cyber Diligence to investigate. Our response team began gathering facts about the subject individual and his capabilities.

Challenge: It was determined that we were dealing with a sophisticated insider, who was possibly involved in industrial espionage. There were also eight other researchers working on a particularly important project, so Cyber Diligence needed to quickly ascertain the extent of this individual's activity. We wanted to find out what he was doing, how much he accomplished so far and for whom he was working. Our examination revealed that the subject installed a potent key logger to see if anyone tampers with his computer. Any attempt to peek at the subject employee's computer when he was away from it would be immediately revealed. He also had various hacker tools installed on his laptop in addition to a data scrubber software.

Response: Our team determined that the best approach should be to covertly examine his laptop computer without raising suspicion. A plan was developed to use a Forensic Drive duplicator to obtain a forensic copy of the laptop hard drive without turning the laptop on. Cyber Diligence investigators also covertly installed highly sophisticated Network Forensic collectors on the R&D network to capture electronic evidence as it was traveling over the network switches and wires (data in motion). In addition, sophisticated countermeasures were also deployed on the client's Research and Development server itself to record all activity.

Results: Our initial forensic examination of the laptop revealed no evidence of wrongdoing due to the presence of a data scrubber. It appeared that every day when this subject got home, he ran a scrubber program overnight to clean his hard drive. The drive contained virtually no data anywhere, other than a handful of legitimate files he was working on. As there was no evidence of data theft on the laptop drive, and the mere existence of these programs could be explained as being innocent in many different ways.

Our investigators' initial determination was that there was nothing incriminating about this individual's work on his computer. However his observed activities were suspicious enough and we had to find the "smoking gun" in other ways. The Network Forensics collector proved to be fruitful. After a week of collecting network traffic, Cyber Diligence analyzed the collected data and recovered evidence that this individual was attempting to misappropriate company trade secrets.

The potential loss to the client was estimated to be over \$100 million.

Cyber Diligence offers IT/Computer security awareness training for all levels of employees; and we offer capabilities for computer and network forensics. Contact us at (516) 342-9378 www.CyberDiligence.com

ABOUT CYBER DILIGENCE, INC.

Founded by Mr. Yalkin Demirkaya (NYPD Retired) Cyber Diligence is comprised of highly trained investigators who are world-recognized experts in information security (INFOSEC), Incident Response, Investigations and security management. Cyber Diligence Investigators are experienced criminal investigators who are also skilled at deploying sophisticated state-of-the-art tools to combat Information Technology crimes and to counter intrusions that compromise valuable corporate assets.

Cyber Diligence specializes in conducting highly sensitive covert internal investigations. Our expertise includes:

- Insider abuse detection
- Investigations into actual or suspected industrial espionage
- Electronic Discovery Services
- Litigation Support/Expert Testimony
- Incident Response
- Computer Forensics
- Network Forensics
- IT Security Assessments
- Intellectual Property Protection
- Malicious activities and other forms of misconduct or corporate compliance violations.
- Counter-Surveillance Services (Technical Surveillance Counter Measures)

Cyber Diligence is a licensed Private Investigations firm, whose investigative team members are former law enforcement investigators and commanders. They possess over 140 years of investigative experience and have successfully investigated many high level industrial espionage cases in the United States and abroad.

WHY CYBER DILIGENCE?

1. We have the knowledge, skills and experience.
2. We have a state-of-the-art lab equipped with the latest computer and network forensic tools to tackle any cyber security incident. We attack the problem with the right tools.
3. We have a unique IT assessment methodology to assess an organization's IT security posture to protect against internal & external threats.
4. Qualified people with years of computer crime investigative experience ask qualified questions – we trust the answers, but we always verify.
5. We take a realistic approach to your business, understanding your culture to secure your business with common sense solutions.

Contact Us: info@CyberDiligence.com

WWW.CyberDiligence.com Phone: 516-342-9378 | Fax: 516-605-0862 | 575 Underhill Blvd. Suite 209 Syosset, NY 11791