

IP Theft Seriously Impacts a Business

Lessons Learned from the Real World

The management of a regional company providing services to the government was understandably concerned when it lost an important government contract to an unknown start-up. The concern grew to alarm, however, when the company realized that the start-up was staffed entirely by its own recently departed employees. The client company suspected the former employees of using proprietary information to bid for and provide services to the government agency, as well as inside knowledge of the contract bidding price, to “steal the deal.” The company retained counsel but they needed hard proof to confirm their suspicions. They hired counsel but also needed the experience and skills to investigate the theft of IP from computer sources and the digital evidence to make a strong case against their former employees. They needed digital forensics expertise to conduct a comprehensive investigation in the matter.

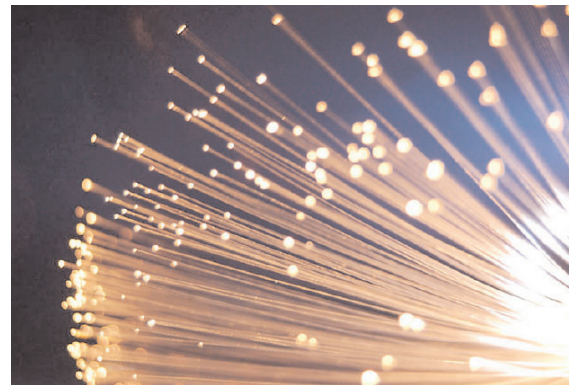
During the course of the investigation and discovery, a forensics examination was performed on the suspects’ former work computers. Through analysis of link files, metadata, event logs and the recovery of unallocated e-mail and document fragments, the investigation was able to establish that the suspects had used web-based e-mail accounts to circumvent the company’s e-mail system and communicate about creating the new company, had accessed and copied information from restricted network locations, and had burned key information to CD, all shortly before leaving the company. The findings were presented in expert testimony that was used by counsel to gain court-ordered access to the work and home computers of the former employees in their new place of business.

With access to the suspects’ current computers, the investigation confirmed that the suspects had indeed used the client company’s proprietary information to create service offerings and a successful bid to the government agency. In addition, the investigation uncovered an effort by the former employees to destroy information by deleting data and running a de-fragmentation program. The client company won back its contract thanks to the conclusions presented in expert reports and testimony.

Turning Information into Intelligence

As we have seen in the above real-world example, organizations are faced with numerous issues that can quickly compromise their business and reputation. Top among these issues are emerging digital threats that include employee malfeasance, computer intrusions, data breaches, theft of intellectually property, civil disputes and others like government and regulatory inquiries; all which can arise without notice. When this happens you need to know quickly how to identify and lock down potential sources of digital evidence on all IT assets including mobile and telephony devices. How best to preserve and most importantly, how best to use it for your end goals becomes the major focus of a successful strategy.

Digital forensics, e-discovery and investigative techniques are integral parts of a complete enterprise risk and information assurance discipline that help enterprises deal with security breaches, policy violations, and legal compliance preservation obligations more effectively. Organizations that prepare their IT systems as a potential source of evidence put themselves in a better position to minimize the costs and penalties



associated with exposure of sensitive data, civil discovery requests, and regulatory investigations. To accomplish this, organizations should look for assistance from qualified forensics experts who can conduct sophisticated digital investigations and deal with constantly changing and complex IT environments with the experience to effectively combat the increasing sophistication of those intent on fraud, deception, crime or harm.

Complementing the HRR Approach

Stroz Friedberg, LLC is a technical and consulting services firm specializing in digital forensics, e-discovery and corporate investigations. They combine a deep understanding of legal issues and investigative techniques with an unparalleled acumen in technology; proven at the fore-front of digital forensics and electronic data preservation in some of the largest and most important corporate and government cases. **h**

The Firm’s partnership with Stroz Friedberg gives us the capability to further assist our clients. To learn more about Stroz Friedberg’s capabilities, visit www.strozllc.com or call (212) 981-6540.

Edward M. Stroz, Co-President, Stroz Friedberg, LLC, has over 20 years of experience in law enforcement, computer crimes investigations and digital forensics. In 2000 he founded Stroz Friedberg after 16 years as an FBI Special Agent. He is sought for his expertise in successfully leading complex investigations for digital fraud and cyber-crime issues facing businesses today.