Security needs drive cyberforensics

November 23 2010, By Byron Acohido

Cyberforensics, the science of finding and securing digital evidence buried deep within company networks, is fast emerging as a global industry.

Three major players are in the vanguard. PricewaterhouseCoopers has recently hired several former law enforcement agents and prosecutors to supplement its cyberforensic services, which already have 3,000 employees and 55 labs in 37 countries.

Verizon Business - supplier of communications, networking and security technologies to large organizations - has pumped more than $50 million into cyberforensics-related services in the past two years. That includes setting up a state-of-the-art hygienic lab to examine computer circuit boards.

And Stroz Friedberg, a private CSI-like company founded by an ex-FBI agent and an ex-U.S. Attorney, recently received a $115 million investment from private-equity firm New Mountain Capital to open new offices across the U.S., Europe and Asia.

Demand for cyberforensics is being driven by "the proliferation and complexity of security issues companies are facing," says Alok Singh, New Mountain's managing director. "Issues of data security and integrity are critical for all companies around the world."

Large organizations increasingly need expert guidance preserving and extracting digital records, such as e-mail and copies of sensitive documents, for civil lawsuits and regulatory audits. They also increasingly need help getting to the bottom of security breaches.

U.S. Internet crime losses reached $560 million in 2009, up from $265 million in 2008, says the Federal Deposit Insurance Corporation. Research firm Market Research Media estimates that the federal government will spend $55 billion from now through 2015 on cybersecurity. Globally, a recent study by the Computing Technology Industry Association, a nonprofit trade group, found that 63 percent of large organizations surveyed in 10 nations experienced at least one security incident in the past 12 months, with 45 percent of those incidents classified as serious.

Much like the CSI investigators portrayed on TV, cyberforensics sleuths preserve the crime scene and use their training, experience and intuition to ferret out crucial evidence. But instead of looking for fingerprints, DNA and ballistics, they hunt for "subtle data attributes inside company networks that have been changed or altered," says Ed Stroz, ex-FBI agent and co-founder of Stroz Friedberg.

PricewaterhouseCoopers forensics director Kim Peretti, a former Justice Department litigator, says the hunt can become intricate. "Looking for breach indicators is really more of an art than a science," Peretti says. "The more you do these type of investigations, the more you know where to look and what to look for."

Citation: Security needs drive cyberforensics (2010, November 23) retrieved 26 April 2024 from https://phys.org/news/2010-11-cyberforensics.html