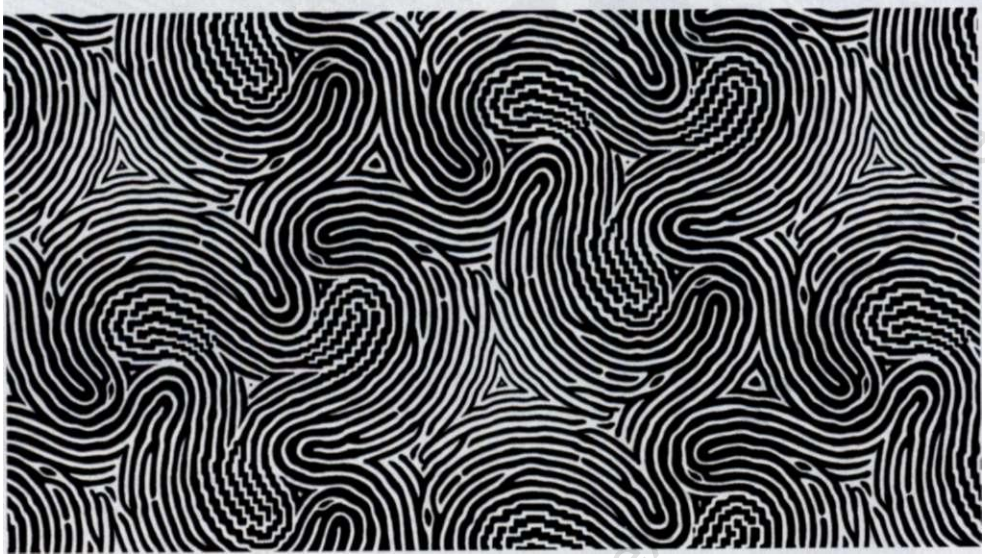
TECH@WORK

CSI for Companies Burned by Hackers

Firms are increasingly turning to cybercrime forensics experts like STROZ FRIEDBERG when they've been the target of an attack. *by Michal Lev-Ram*



IN A TINY LAB on the 24th floor of a high-rise in downtown San Francisco, a couple of forensic examiners are piecing together evidence. But there aren't any blood or gunpowder samples. Instead, there are hard drives, traces of deleted e-mails, and server logs to sift.

The examiners—who asked not to be named—are digital forensics experts at Stroz Friedberg, one of a handful of cybercrime first responders that companies turn to when they've been hacked. As the scope and size of cyberattacks have grown, so has Stroz Friedberg's business. Though the private company does not disclose its numbers, it says revenue rose 18% from 2011 to 2012, as the likes of Facebook and Brocade Communications Systems engaged the firm to investigate cases of intellectual-property theft, denial-of-service attacks, embezzlement, and myriad other cybercrimes.

"There's much more awareness now," says James Aquilina, executive managing director at Stroz Friedberg and a former federal prosecutor with the criminal division of the U.S. Attorney's Office in Los Angeles. "Even when budgets are tight, companies are spending more on security," he adds.

Edward Stroz, former head of the FBI's computer crime squad in New York, and former federal prosecutor Eric Friedberg started the consultancy in 2000. By 2010 it had secured $115 million from private equity firm New Mountain Capital. Stroz Friedberg now operates 13 offices worldwide—including branches in New York City, Hong Kong, and London—and employs over 300 people. Many of them are digital forensics specialists who keep a travel kit with them at all times—if a frantic customer call comes in, they quickly hop on a plane.

But while companies often move quickly once they know they've been attacked, discovering they've been targeted can take some time. According to a recent report from Verizon, 66% of breaches take months or longer to detect. Once discovered, an attack can usually be contained within days. That's where Stroz Friedberg and its competitors come in. Companies look to them to determine the "vector" of attack—how an intruder infiltrated their data and what he accessed. They are also tasked with rebuilding computer systems and, increasingly, helping guard against future attacks.

Of course, there is no way to fend off all intruders. As security experts like to say, it's no longer a question of if a cyberattack will take place, but when. That means no shortage of future investigations—and mountains of digital evidence—for Stroz Friedberg's anonymous examiners to comb through.

THREE OTHER DIGITAL SLEUTHS

MANDIANT
Started by a retired Air Force officer, Mandiant recently released an explosive report on Chinese hacking.

VERIZON'S RISK TEAM
The telecom giant's team specializes in digital forensics and "malcode" analysis. It publishes an annual report on data-breach investigations.

KROLL ADVISORY SOLUTIONS
This large cybersecurity investigation specialist also helps companies run background checks on prospective employees.

Fonte: Fortune, Amsterdan, v. 167, n. 8, p. 30, 10 Jun. 2013.