



August 2002 - Cover Story  
**Computer Forensics**  
**Detecting the Imprint**  
by Illena Armstrong



Ferretting out evidentiary imprints left behind by cybercriminals is a tall order in the virtual world of zeros and ones. But, this digital realm is proving a ripe and ready stomping ground for crooks of all kinds.

Electronic crime's appeal runs the gamut, as exemplified by some recent illegal acts:

- Discovered in June, an unidentified person – believed to be a Chinese national – hacked into 21

accounts at the Development Bank of Singapore Ltd. He reportedly transferred thousands of dollars to his own account, according to a Singapore Sunday Times newspaper article.

- A man, possibly tied to the Russian mafia, was arrested in June for allegedly installing keystroke-capturing software onto computers at various universities in the U.S. He was allegedly seeking to capture credit card numbers and other personal data, according to a piece in The Chronicle of Higher Education.
- After receiving tips from the Federal Bureau of Investigation (FBI), Polish police say they have tracked down the PC used by the hacker who gained illegal access to NASA's computer network, causing some \$1 million in damage, according to recent Polish television reports. If arrested and charged with the crime, the man – a Polish citizen and known computer expert – could be sentenced with up to eight years in jail under the country's cybercrime legislation. This does not take into account the possibility of the alleged hacker being extradited to the U.S.

In Riptech's Internet Security Threat Report, released in July 2002, about 20 percent of the several hundred companies monitored by the service provider experienced at least one severe attack during the six-month analysis period that started in January. Adding to these attack

types, which seem to be occurring at a more frequent pace, fears of cyberterrorist assaults have heightened since the Sept. 11 strikes. A Business Software Alliance survey in June 2002, commissioned by Entrust, revealed that 49 percent of the 395 IT professionals surveyed believe that the U.S. federal government is highly vulnerable to attacks by cyberterrorists. Further, one third of these say they think such attacks are very likely to happen within the next year.

Given the innumerable digital threats plaguing organizations today, experts say they have seen an increased interest in the merits of computer forensics technology – from forensics pre- and post-planning to the collection of electronic evidence for purposes of formal litigation and simple internal investigations. At the same time, however, Meta Group estimates that only a mere five percent of its corporate clients use computer forensics tools or techniques.

“Computer forensics is an area where many companies fear to tread – until they have to,” says Michael Bacon, evangelist and principal of archolutions.com, an architectural solutions company based in the U.K. “It requires specialist training, not only in technology, but also in evidence gathering and presentation in court. Few corporates are prepared to invest the time and money in their own staff to train them up.”

Still, says Bacon, organizations are seeing the value of computer forensics procedures for business activities, such as recovering data on systems used by former employees or conducting internal investigations – “often into abuse of acceptable use policies.” Too, they find such forensics technologies aid in supporting “some aspects of corporate governance.”

Just acknowledging the volume of data stored on networks should be enough reason to prompt enterprises to begin examining the validity of using forensics, says Clive Carmichael-Jones, operations director at Vogon International, a developer of computer forensics technology. “Key to understanding the role of computer forensics in the modern corporate organization is the fact that virtually all documents that are handled today originate in electronic form. From this realization comes the logical conclusion that the destruction of paper documentation is almost incidental in terms of consequential impact next to the intent, and subsequent attempts made, to destroy the original electronic data,” he says.

As part of this logic, a company must realize that in support of the security policies and the various security technologies they have in place, computer forensics provides the means of investigation when these plans and tools are compromised in some way. As an example, Alyn Hockey, vice president of future products for Clearswift in the U.K., explains, “Monitoring products act as an early warning sign, alerting management to the possibility that they need to use forensics to investigate the source of a possible threat more thoroughly.”

Just as prevention, planning and deployment of security tools are necessary steps for businesses of all sizes to take these days, so too is the use of computer forensics tools and plans. "The ability to respond to an incident, understand its causes and effects and take the appropriate remedial actions, is fundamental to effective information security," says Robert Brown, technical director for DataSec Limited in the U.K.

## Taking Steps

Ensuring that a company is on the right computer forensics path begins with an understanding of the tools and protocols associated with this area of infosec. This is an important move since forensics can mean many things to many people.

"Forensics, used to its potential, can provide both pre- and post-event benefits," says John Suit, CTO of SilentRunner. "Forensics enables IT security staff to understand who is using the network, how they are using the network, and for what purposes. If a violation occurs, from internal or external sources, computer forensics is the cornerstone of reconstructing the event that took place. The focus is on obtaining and analyzing information. Using technology in combination with policy, corporate investigative units are fulfilling their models of 'protect, detect and respond,' while rounding out their models with corporate accountability."

Hackers seeking to compromise web applications "don't schedule their movements," says Ory Segal, a security specialist and developer in Sanctum, Inc.'s security group. He believes that in today's world of mission-critical, web-enabled information, it's vital for IT professionals to have full insight into the activity on their sites. "Web forensics," he says, "has become a vital Internet security component" in this analysis.

The addition of the computer forensics component to business planning helps in building and maintaining a strong security posture, notes Larry Lunetta, vice president of marketing for ArcSight, Inc. All the "rubble" of the various security tools most companies have in-house – such as IDS, firewalls, and more, contain "clues to how the attack happened, why it was successful, and how to detect and prevent similar incidents in the future."

One of the best tactics for which computer forensics techniques and technologies should be used is the simple protection and recovery of information, says Adrian Reid, managing director of DataSec. In the U.K. alone, 76 percent of corporations store critical or sensitive data on their networks, according to the Department of Trade and Industry (DTI). As such, organizations must take measures to protect this information and investigate an incident when it involves this data. "[We have] seen an increase in the number of investigations instigated by corporate victims and a trend towards an aggressive approach to recovering stolen information, which might involve court orders to

seize and examine computers that allegedly hold stolen data," Reid says. "Basic forensic principles that lead to appropriate first action being taken when an incident occurs, and an increased likelihood that information will be recovered, preserved and admissible as evidence, are beginning to be implemented in the corporate world."

To execute this process properly, planning is integral, says Larry Kanter, a partner with Ernst & Young who manages legal technical services for the U.S. Such planning, he says, must begin with senior management, because IT security and forensic technology plays across all departments. To begin the process, the general counsel's office must initiate and maintain an open dialogue with the IT department in order to establish appropriate policies that address such issues as document retention, email/Internet usage, and more.

From there, companies can take measures which will be quite helpful when something does occur, says Barry Stauffer, CEO of Corbett Technologies, Inc. in Virginia. Such pre-planning includes:

- Setting up a retainer contract with a business that specializes in computer forensics in advance of major events. A contract of this kind should offer a 24/7 guaranteed response.
- Educating system administrators and/or other IT professionals on how they should respond to an incident before the forensics experts arrive. This is pivotal so that these employees avoid taking actions that "pollute the evidence before the computer forensics team arrives," making it inadmissible in a court setting or impeding the team from discovering important information.
- "Having the network architecture include a system that logs all data from most network devices."

To be sure, adds Cliff May, principal consultant with Integralis in the U.K., setting up an incident management plan will be helpful in preventing panicked behaviors. An important part of such a plan involves designating certain people with the responsibility to monitor and report on anomalous behaviors. By defining specific roles such as these for employees, companies can offer adequate training on the various forensics technologies and how to properly deal with potential digital evidence so it can hold water in a courtroom.

"The most important lesson that companies should consider is not to panic, jump to conclusions or make accusations until they know all of the facts. Often, the issue is only the tip of the iceberg and you need to dig deep to find out exactly what has gone on," he says. "But, companies are not doing this. [They are] still too reactive, dealing with issues as they come up. Pressure makes people do the wrong thing. If you have a procedure in place, then this won't happen, as you'll have primary [people who are responsible]. And, if they aren't around, there will be back-up options, as well."

Such awareness and definition of roles should cover everyone from end-users to the response staff, notes Ben Rothke, senior security

architect with QinetiQ Trusted Information Management, Inc. By having end-user awareness policies, incident response staff and a comprehensive set of incident response policies and procedures in place, "an organization has a good chance of success." (Read more details on each of these components in the accompanying sidebar Parts of the Plan at the foot of this page.)

Also, as part of the proactive mode, says Stauffer of Corbett Technologies, computer forensics tools can be used to do the following. Examine corporate systems, first, to see if an incident is about to take place. For example, tools could be used to find out if a disgruntled employee is planning to commit corporate espionage by selling secrets to competitors. Then, examine corporate systems to see if an incident is taking place now, such as discovering that "a trusted ... employee is running [a] business via the corporate link to the Internet." As for the role of being responsive, forensics tools "can be utilized to ... rescue ... some corporate entity that knows their network has been violated in some manner," he notes.

Moving onto the reactive mode, DataSec's Brown says that there are quite a few specific actions to take when a hacking incident takes place. A few of his main steps are shown in the accompanying sidebar When You've Been Hacked. He notes that organizations cannot underestimate the importance of pre-planning. The time to consider what actions to take should not happen when the company has been hacked.

"By preparing a planned response, the reaction can be swift and coordinated rather than blind panic," he explains. "According to the CERT Coordination Center, hacking incidents are on the rise. During 2001 alone they dealt with over 52,000 incidents, a 160 percent increase on the previous year. With such a dramatic increase it is inevitable that many companies will not have a prepared response to deal with an intrusion. However, the growing press coverage of high-profile incidents is helping to alert businesses to the danger that exists and, hopefully, spur them on to build their defenses and prepare for the inevitable first successful attack."

## Working the System

All of these steps that experts suggest are inordinately helpful to any forensics investigation. However, adds Reid of DataSec, many companies still fail to report hacks and other digital crimes to police agencies. As such, some investigative bodies are attempting to create systems that will encourage organizations to report cybercrimes. For example, Reid says that the U.K.'s National Hi-Tech Crime Unit is reviewing "a crime-reporting system that will protect the identity of the corporate victim." Not operating yet, this type of system could "receive objections" from legal officials, though.

Another problem with making reports to law enforcement is that they may lack the resources – money, equipment, trained personnel and

more, to properly investigate a computer crime, says John Wiechman, president of TLSI, a computer forensics organization in Texas. While this may be true, adds Dave Schultz, electronic evidence legal consultant for Kroll Ontrack, investigators in most technologically advanced countries are beginning to get a handle on cases involving digital evidence. Typically in the U.S., the federal agencies are far more advanced than local bodies, he notes, but all are making changes for the best.

Whether companies are worried about policing agencies' expertise or not, sometimes matters little in many regions. In these areas, it is not optional to report a criminal act, notes Alan Sternecker, a retired FBI agent who now owns consultancy Risk Management Associates. Due to this fact and others, it is important that executives decide before an incident occurs whether or not it is appropriate for them to report it. Also, before something goes down, Sternecker suggests that executives "establish liaison with local, state or federal law enforcement authorities." By doing this, organizations can learn "under what circumstances [law enforcement agencies] wish to be notified and how they wish to have evidence handled in preparation for their arrival." And while it may be true that some policing agencies may still be grappling with investigations, most are quite familiar with the role of such digital equipment in committing crimes.

"Agents, officers and technicians have actively sought specialized training in collecting, processing, storage and presentation of digital evidence. There are many academies sponsored by private and public sectors that have been providing this type of training for many years," notes Sternecker. "In smaller jurisdictions, there are working groups and task forces to address technical issues. As always, it is the responsibility of law enforcement agencies to upgrade their training and personnel to address emerging technologies impacting crime. Agencies are very aware that exchanging information will greatly assist in addressing crimes that are traditional or white color in nature. I think most agencies are taking steps in that direction as fast as their budgets and legislatures will allow."

Above and beyond reporting incidents to various police agencies, Jack Wiles, president of TheTrainingCo., says that companies in the United States also have the option to go to one of the local Infragard chapters or the Electronic Crimes Task Force. The former is an FBI program and the latter a U.S. Secret Service program. Both groups combine the knowledge and expertise of their respective agencies and business members. Similar organizations exist in other countries.

## **Crossing the Lines**

"The police find it easier to prosecute speeders than electronic crime – cynical, but true," maintains Bacon. "More countries are setting up specialist units to investigate electronic crime, and this should become the norm in all countries over time. However, as the balance shifts in favor of the police – as they understand more about how to investigate

and prosecute successfully – the criminals will switch to other forms of crime. Lawmakers and enforcers will always be on the back foot. I use the analogy of a motorway, the digital highway; the criminals are racing up the outside lane in a stolen Jaguar, [people] like myself are driving their company cars in the middle lane flashing our lights and blowing our horns trying to attract attention. [Meanwhile,] the users are pootling along in the inside lane towing their caravans, [and] manufacturers are pulled up on the hard shoulder tinkering with the engine, while the lawmakers are stuck in traffic jams in the city center [and] the police ... [are pulling over] cars for not displaying a tax [tag] on the near-side [windshield].”

When cybercriminal reports cross international borders, organizations must recognize that policing agencies all over the globe are doing their best to work together to bring Internet crooks to justice, however. “Countries are already working together to track and destroy cybercrime,” says Clearswift’s Hockey. “There was a global example of this recently when agencies from an array of countries, including the National Hi-Tech Crime Unit from the U.K., worked together to smash a child pornography ring.”

In addition to U.K. and U.S. agencies making great strides in computer inspections, Scandinavian countries and Canada are also doing quite well in efforts to spearhead international investigations, says John Patzakis, president and general counsel to Guidance Software in the U.S. While these countries and others are trying to crack cases together when necessary, there are still problems in pursuing criminal and civil investigations involving digital evidence when some countries lack cybercrime laws or have no standing investigative agreements with others.

No matter if hacked by locals or hit by those from foreign soils, notes Integralis’ May, it is important for organizations think about filing a report. “They should be reporting all crimes of this nature. The police will help in these matters, but companies need to be more open and come to them when these incidents take place,” he maintains. The problem arises when crime must be tracked down into developing nations, since laws from country to country differ greatly. For instance, in some countries penetration testing is illegal, or legislation, such as the Computer Misuse Act in the U.K., disallows you from accessing information that might be critical to an investigation.

“A major problem that policing agencies have from a global perspective is the lack of any international laws on cybercrime,” says Corbett Technologies’ Stauffer. “This is being worked on, but currently hacking into another nation’s computers is encouraged and kept legal by some governments while totally illegal in other countries. Therefore, to prepare to take on electronic crime committed by white collar and traditional criminals, the first major thing that is needed is solid international laws that focus on cybercrime. Once we have that, we need a solid computer forensics training program for these agencies, with the necessary budget.”

But, achieving this will take time, commitment and much effort on the part of agencies. Too, political hurdles that often impede development of such international cooperation will need to be overcome.

"As in many things, law enforcement and judicial systems perform to the best of their abilities and are frequently limited by budgets, treaties and legislatures. I sincerely believe that most agencies are acutely aware of the impact of digital evidence in criminal and civil investigations," says Sterneckert. "Most are actively seeking training, expertise and resources to address these matters."

In the meantime, says Simon Platt, national partner in charge of computer forensics with Deloitte & Touche, since cybercrime knows no physical boundaries, "any step for countries to take to work together is in the right direction."

## What to Remember

"Companies are painfully aware that everything they [have done] was probably created on a computer," says Ernst & Young's Kanter. "This data virtually permeates the entire organization."

As more and more data is stored in the digital medium, notes Ian Hameroff, director of security solutions for Computer Associates, it is important that companies enlist the help of the many computer forensics tools available to them. They must establish policies before an incident happens, ensure they get the right personnel involved and that these folks have been trained so that the company can learn from the attack and recover from it.

To be sure, they must call in the experts to help with collection and preservation of evidence, if they don't have a team of their own in-house experts on staff. In retaining sound professionals, Vagon's Tony Dearsley, computer investigations manager, says companies must count on a "reputable firm with a proven track record and ... strong technical support."

And, says archolutions.com's Bacon, pre-planning is the step that makes investigations of all kinds run smoothly. "Identify the internal or external experts, set up a means of calling them, and work this sort of incident planning into your crisis plan," he says.

Too, this step is key because "computers are playing an increasingly important role for the criminal as data storage devices and instruments of unlawful behavior," says Sterneckert. "It's important to note that law enforcement agencies don't usually deal with civil and administrative issues that may be important to business and government organizations. Consequently, having computer forensic resources available is gaining importance. We have replaced filing cabinets and communication systems with computers, servers and related equipment. Our organizational need to audit, monitor and, at times, research these devices and data, greatly depends upon

technology and forensic experts.”

Businesses, notes SilentRunner’s Suit, are comprehending this notion and are beginning to depend on such technology to speed up and protect their various technological processes, but also meet outside legal and regulatory mandates.

“Organizations should have defined policies around incident handling,” Suit warns. “Regardless of whether an organization chooses to call law enforcement or just clean up the broken glass, it is essential it has appropriate processes in place to identify the issue and respond to it all levels in the organization, from executive to technical.”

## Information Extra

This listing is a sampling of organizations involved in the forensics arena.

**archolutions.com**  
[www.archolutions.com](http://www.archolutions.com)

**ArcSight, Inc.**  
[www.arcsight.com](http://www.arcsight.com)

**Clearswift Corporation**  
[www.clearswift.com](http://www.clearswift.com)

**Computer Associates**  
[www.ca.com](http://www.ca.com)

**Corbett Technologies, Inc.**  
[www.corbett-tech.com](http://www.corbett-tech.com)

**DataSec Ltd.**  
[www.datasec.co.uk](http://www.datasec.co.uk)

**Deloitte & Touche**  
[www.deloitte.com](http://www.deloitte.com)

**Ernst & Young**  
[www.ey.com](http://www.ey.com)

**Guidance Software**  
[www.guidancesoftware.com](http://www.guidancesoftware.com)

**Infragard**  
[www.infragard.net](http://www.infragard.net)

**Integralis**

[www.integralis.com](http://www.integralis.com)

**Kroll Ontrack**  
[www.ontrack.com](http://www.ontrack.com)

**New Technologies, Inc.**  
[www.forensics-intl.com](http://www.forensics-intl.com)

**PentaSafe Security Technologies, Inc.**  
[www.pentasafer.com](http://www.pentasafer.com)

**QinetiQ Trusted Information  
Management, Inc.**  
[www.qinetiq.com](http://www.qinetiq.com)

**Sanctum, Inc.**  
[www.sanctuminc.com](http://www.sanctuminc.com)

**SavvyData**  
[www.savvydata.com](http://www.savvydata.com)

**SilentRunner**  
[www.silentrunner.com](http://www.silentrunner.com)

**TheTrainingCo.**  
[www.thetrainingco.com](http://www.thetrainingco.com)

**TLSI**  
[www.tlsi.net](http://www.tlsi.net)

**U.K. National Hi-Tech Crime Unit**  
[www.nationalcrimesquad.police.uk/nhtcu](http://www.nationalcrimesquad.police.uk/nhtcu)

**U.S. Electronic Crimes Task Force**  
[www.ectaskforce.org](http://www.ectaskforce.org)

**Vogon International**  
[www.vogon-international.com](http://www.vogon-international.com)

**Vordel**  
[www.vordel.com](http://www.vordel.com)

**WetStone Technologies, Inc.**  
[www.wetstonetech.com](http://www.wetstonetech.com)