

## New World, Old Problems

Computer and network technology have improved the lives of most people and created entire new industries. Unfortunately, this technology is of equal use to criminals – moving traditional crimes to new media and creating new crimes to exploit the new technologies and businesses. Some forms of crime that could be managed locally can now be distributed globally. This widespread distribution creates challenges for crime prevention, identification, and investigation, as well as complications in jurisdiction and for prosecution. Additionally, the automation of major national utility and economic infrastructures has enabled new threats that require coordinated response from industry, law enforcement, military, and intelligence organizations.

## A Framework for the Future

Law enforcement has been compelled to respond to computer crimes on a case-by-case basis. Innovative analytic and investigative techniques have been developed to meet specific challenges. These forensic techniques must be part of an overall framework to ensure that law enforcement can move towards preemption and prevention of computer crime as well as more effective prosecution:

- **Patrol, Prevention, and Public Health:** The best strategy for law enforcement is to stop computer crime before it occurs. Early warning systems, tools to escalate anomalous logging events, virus and malicious code protection mechanisms, and training and awareness all need to be integrated into a comprehensive, pervasive security program to prevent crime. ITGlobalSecure believes that its **Internet Immune System<sup>SM</sup>** is a key part of building an IT infrastructure that can prevent and minimize the impact of computer crime.
- **On-line Investigation:** Surveillance, both the passive monitoring of computers and networks as well as the active installation of hardware and software to collect evidence, is at the heart of capturing and prosecuting computer criminals. New solutions are needed to ensure that evidence is collected lawfully and that it can be presented in court. Particular challenges are the proliferation and rapid evolution of computer and network technologies (moving from the Internet to broadband and numerous wireless systems) making the cost of developing, training, staffing, and operating an investigation operation often prohibitive. The expansion of service-based solutions, collaboration, and outsourcing in a manner that preserves the quality and control of an investigation is a major challenge that will need to be solved to control costs.
- **Forensic Analysis & Evidence Development:** Turning raw surveillance data as well as media, logs, and other materials into evidence that can be used by prosecutors and presented in court is a key task. Formal methodologies need to be developed and laboratories certified just as certain medical and other evidence is processed today to ensure the proper chain of custody of evidence and prevent its modification to guarantee that it can be used in court. In-house laboratories will require standard techniques, training, and handling procedures to ensure quality, completeness, and usability.
- **Oversight, Intelligence Analysis, and Management:** The scope and complexity of computer crime requires a systematic approach to synthesize the multiple evidence collection systems. Improvements can result from integrating on-line and off-line law enforcement intelligence collection systems for multiple crimes within a Computer Crime Management Information System (CCMIS). CCMIS will help isolate real crimes from computer vandalism, identify problem sites and services, and otherwise bring coherence to the complexities of both computer systems and networks as well as business, utilities, and other elements in a jurisdiction's IT infrastructure.

- **Coordination and Liaison:** Problems of jurisdiction and cooperation plague computer crime investigations. Means must be established to share intelligence while maintaining security and rapidly respond to incidents anywhere on the globe while protecting sovereignty and local autonomy. Creating the technical tools and solutions will be a challenge – developing the trust and cooperation to make such systems effective will be daunting.
- **Court Presentation:** Ultimately, evidence must be presented to a judge and jury. The complexity of explaining evidence and its collection, much less the crime, to these individuals will benefit from use of the same technology that enabled the electronic crime, itself. Visualization techniques, multimedia presentations, and expert witnesses will turn the tide in many of these computer crime cases.

---

## Facing the Challenge

Law enforcement professionals confronting computer crime face many new and unique challenges: global criminals, the proliferation and sophistication of advanced attack tools, a world in which even bored adolescents can casually commit serious computer crimes, and the complexity and rapid evolution of information technology. Crimes are not reported and criminals get lucrative employment contracts from their victims. New strategies must be developed. Existing security tools address basic network and operating system vulnerabilities, but the valuable assets to companies, countries, and criminals lie in the proprietary databases and business applications (Oracle, SAP, DB2) as well as unique business applications and custom network infrastructures. Until law enforcement can fight criminals in all of these new and existing technologies, they will be fail to see or be unable to realize victories against these new threats using new technologies.

If you are interested in help protecting your IT infrastructure or developing solutions to IT law enforcement challenges, contact:

IT GLOBALSECURE INC.  
IT SECURITY SOLUTIONS LLC (Asia)  
Phone: +1.202.332.5878  
Fax: +1.202.478.1743  
Email: [info@itglobalsecure.com](mailto:info@itglobalsecure.com)  
[www.itglobalsecure.com](http://www.itglobalsecure.com)