

The Role of Ethics in Information Technology (IT) Security
Peter J. Hillier, Senior Consultant,
CGI InfoSec Centre Of Expertise

Reported by Dave Edmunds

Mr. Hillier commenced by stating that the objectives of his presentation were to discuss some of the ethical issues in IT Security, and what are our responsibilities. He defined ethics as understanding how your actions affect other people, knowing what is right and wrong, and taking personal responsibility for your actions. In the context of IT security, ethical issues are no different than ethical behaviour in the physical world, but they become more challenging because hundreds of millions of people worldwide use computing resource, seemingly under some guise of anonymity. This interaction can have both positive and negative effects. The key ethical considerations revolve about the fact that we all comprise the internal, external user base; we are all personally responsible and accountable; and we have children who are either sharing or have their own personal computers at home or at school.

Mr. Hillier displayed a list of various ethical issues (plagiarism, inappropriate use, social engineering, cyber stalking, piracy, hacking [cracking], viruses, worms, etc, flaming and hate mail, meeting people, pornography) arising from the use of the Internet. He said that the billions of dollars spent each year on IT security software, hardware, programs, and services; such as intrusion detection systems, content filtering, anti-virus, anti-spam, and others; do little more than react to security problems. He quoted an analysis by Datamonitor predicting that global spending on enterprise security products will rise to \$13.5 billion in 2006, spurred on by the need for security administrators to manage an increasing number of new threats. He questioned whether much of this expenditure really dealt with the source of security problems. He suggested that children are responsible for much of the unethical activity on the Web, and therefore, awareness of IT ethics should begin during childhood before bad ethical habits move into the workplace.

Discussing plagiarism, Mr. Hillier stated that schools, universities, and government bodies have done little to educate students about the impact of unethical computer and Internet use. Instead, they have taken a particularly reactive approach to what they consider to be an onslaught of plagiarism by subjecting student papers to plagiarism reviews. For many students, the principle of "fair use" is a foreign concept, and the ready availability of information on the Internet makes it easier for them to use someone else's work without giving the author appropriate credit. He has concluded that so many students developed these bad habits because they don't understand the right and wrong ways to use the resources that are given to them.

Various surveys indicate that employees with Internet access at work spend an average of one hour per day surfing the Internet for non-work related reasons. In an organization with 25,000 employees the cost to that organization would be over \$100 million in lost productivity each year. For less than \$400,000 a year, that same organization could put together a package of six courses that would educate employees about appropriate Internet use. If those courses enabled the organization to reduce inappropriate use by 25 percent, it would save \$28 million in lost time.