EXECUTIVE SUMMARY

In the digital era, crime presents several challenges to individuals, public and private organisations, the economy and society as a whole. With the economic revolution in information technology, new types of crime have emerged and traditional crimes have been enhanced.

Information and communications technologies (ICT) enabled crime happens in both the physical and virtual worlds. In addition, economies no longer operate within geographical limits and national boundaries, and concomitant crime is not restricted to a specific territory. The internet is trans-border in nature and confounds the territorial and nationalistic nature of law enforcement. The consequences of criminal behaviour are more far reaching than before, while in contrast, laws combating crime are generally confined to individual states or trading blocks, such as the European Union.

New legislation and international conventions need to address this, and South Africa has embarked upon a process to create such a framework. At a global level, some of the most significant policy influences come from the: International Labour Organisation, International Telecommunications Union, World Bank, Organisation for Economic Co-operation and Development, United Nations Commission of International Trade Law, United Nations Conference of Trade and Development, and World Trade Organisation.

A vast array of organisations, associations, and forums are engaged in e-commerce policy and market development, research, monitoring, enforcement and arbitration. All deal with digital information that can be stolen, destroyed, modified and prevented from flowing.

In a recent global survey on e-fraud in top trans-national organisations, most participants felt that e-fraud was a more likely threat than any of the other types of fraud. Although most respondents felt that their firms could manage the threat of computer fraud, in the year preceding the survey (1999), more than two-thirds of their organisations had suffered from computer fraud, while recovery levels were extremely low. The vast majority was concerned that significant e-fraud could occur and in many instances no explicit policy on reporting e-fraud existed within their organisation.

Arguably, one of the most significant results of the survey was that: over four-fifths of all identified e-frauds were committed by employees, of which one-third was committed by management and half by employees who had been with the organisation for over five years. In South Africa, respondents reported that they were very likely to be susceptible to computer-related fraud committed internally in collusion with organised crime groups.

E-crimes differ from terrestrial crimes in four main ways: they are easy to learn how to commit, they require few resources relative to the potential damage caused, they can be committed in a jurisdiction without being physically present in it, and they are often not clearly illegal. Yet in most countries around the world, existing laws are likely to be unenforceable against such crimes. This means that businesses and governments must rely solely on technical measures to protect themselves. However, self-protection—while essential—is not sufficient to make cyberspace a safe place to conduct business. The rule of law must be enforceable.

Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. A model approach is needed, and provision of a model law will greatly assist in developing countries' attempts to address e-crime. One of the most significant approaches to e-crime is the Council of Europe's Treaty on Cybercrime, which is expected to be operational by 2003. The draft treaty has been described as likely to become the world's standard for fighting online crime. The treaty, to which South Africa is an observer, recommends that member and observer states should adopt legislation and measures with respect to a vast array of offences, and specifies how international co-operation and mutual assistance should be provided with respect to electronic/cybercrime.

South Africa is in the process of enacting its first electronics communications and transactions bill, which will act as the basis of a five-year national e-strategy and seek to promote the readiness of South Africa in respect to electronic transactions. Furthermore, it strives to place the country as a preferred provider and user of electronic transactions in the international market, and is also in line with the European Treaty on Cybercrime.

The e-strategy is quite clear in its expressed desire to solicit the private sector as a partner. It also makes explicit reference to the need to distinguish from, but co-ordinate with, other existing regional, continental and international strategies. One of the more innovative aspects of this bill is the proposed creation of a cybercrime prevention force and specifications of what this force would entail in terms of composition, responsibilities and functions.

Various enforcement agencies are tasked with ensuring that legislation is implemented effectively and fairly. The challenge for enforcement agencies is the prevention of crime in a way that supports the emergence of an enabling environment for e-commerce or the emergence of a knowledge society. At the core of enforcement lie four agencies: the South African Police Service, National Prosecution Authority, the South African Revenue Service, and Customs and Excise. Their current competence base in information and e-enterprise security is difficult to describe or quantify; suffice to say that current initiatives are encouraging, but still in their nascent stages. Strong competence in electronic security exists within South African universities and para-statal research organisations, such as the Council for Scientific and Industrial Research (CSIR).

South Africa's 'Achilles' heel' is the business and financial sector itself, which—based on interviews conducted for this study—is not properly prepared to meet the challenges of e-crime.

South African efforts to reduce the risk of e-crime through legislative, law enforcement, prosecutorial and other initiatives have until recently been piecemeal, but due to the efforts of the Department of Communications they are now heading in the general direction. Both the proposed legislation and statutory bodies that are being planned are in line with international best practice and would place South Africa in tandem with its major trading partners. However, without a greater involvement from the private sector, such legislation alone is unlikely to provide the country with a long-term, robust and effective approach to combating e-crime.