What Do We Really Understand When We Talk About Computer Crime?

Howard Thompson MA I Eng FBCS
Operations Director - Trusted Information Management Ltd

So-called "computer crimes" are increasingly in the news. And why not? It is said that when Willie Sutton, a well-known American bank robber, was asked why he robbed banks he replied that that was where the money was! Nowadays, instead of settling for a few thousand pounds in a bank robbery, those with enough expertise can, it seems, walk away from a computer crime with a good deal more, and seemingly for a good deal less risk. In this new and exciting age information really is power. But of course there is much more to crime than that. So what do we really understand, when we talk about computer crime? In the rise of Cyberspace we have seen a devotion to technical security, whereas we might have been better served by considering criminology. The study of crime in cyberspace has gained little support from the gargantuan information security industry! We need to increase the understanding among IT security managers, policemen, lawyers, lawmakers and even lawbreakers, of what constitutes crime in the cyberspace business environment.

The coming of computer technology has delivered a wide range of advantages and opportunities; some of these, not surprisingly, are criminal in nature. Computers facilitate the commission of what we know as traditional 'old-fashioned' crimes such as theft, damage, fraud or counterfeiting; they also give rise to new mischief's and unwanted and damaging behaviour such as we have come to know as hacking, freaking, spoofing and spamming. It should not be surprising that English criminal law should meet the new challenges posed by the all-pervasive and rapidly expanding use of information technology. But has it? Many unwanted and damaging events cannot be called criminal under the present law. Are we calling these events criminal and indeed providing new offences for the statute book? The Computer Misuse Act (1990), the UK's only real attempt at legislation to be prompted specifically by computer-based criminal activity, seems to have been shown to be mostly ineffective. So why should this be so? Don Parker, a well-known commentator, says that, "if criminals seem to be beating us right and left, no matter what controls we put into our systems, it is because we have failed to understand the way they think. Operational and technical controls in themselves are inadequate because they come from technical experts who do not understand criminal ingenuity and perseverance or the weaknesses or the human factors in computer systems". Crime is a people problem not a technology problem. If we are to meet the challenges we face in this new and e-dynamic world, we need to accept that this is so. We should consider also number of things: the nature of crime in this new age; the security and law enforcement agencies that battle with it daily; and the courts, processes and

procedures which deal with it and its perpetrators.

The very notion of computer security implies that it has evolved to protect us against "cybercrime". Much of the available literature is indeed premised on the basis of that assumption. Many "information security breaches surveys" conducted by multi-national security companies tell us that the survey focused on security breaches arising from premeditated or malicious intent – virus, unauthorised access, fraud, theft, etc. The statistics shown in the report are a summary of the findings in terms of the numbers of incidents and the losses suffered. As in all such surveys of recent years that purport to consider cybercrime, the forms of misuse do not exactly match the legal definitions or concepts of criminal acts.

It has been said that in the future most crimes will involve computers in some way: as a consequence most crime will be cybercrime. If that is so, what will "cybercrime" comprise?" And what will the differences be between a "cybercrime" and what is known as a "crime?" Does this assumption imply that cybercrimes differ from more traditional crimes in ways that will require new laws and the development of new investigative techniques and prosecution processes? Is there indeed something we can call cybercrime? If cybercrimes are to be shown to be a distinct phenomenon, they must differ in some material manner from what we know as traditional crimes. In determining whether cybercrimes actually do exist, we must compare and contrast their nature and their properties with those of traditional crimes. If we can identify substantive and substantial differences between cybercrimes and traditional crimes, we will be able to show how and why these differences are actually realised when the criminal act takes place and define a category of cybercrime. If, on the other hand, we are unable to determine distinct material differences between cybercrimes and traditional crimes, then we would have to conclude that the two are indeed not discrete categories, and that cybercrimes are simply a variation of the existing criminal environment attracting no special need for change to the law or legal process.

So are we are now in a position to undertake an analysis of the differences and similarities inherent in the acts we might describe as cybercrimes – these unwanted troublesome events that are specific to cyberspace - and traditional crimes. Since both cybercrimes and traditional crimes attract a criminal liability, it follows that each category of crime will be predicated on the basic elements that are used to impose such liability. A central question is this: is there a special category of criminal liability for cybercrimes, one that operates on principles different from those we use to impose liability for traditional crimes? In English Law crime may be defined as an act of disobedience to the law forbidden under pain of punishment. The central notion is that nothing is considered to be a crime unless specifically designated to be so. Crimes comprise four elements: the guilty conduct (known as the actus reus), the mental state (known as the mens rea), the attendant circumstances and a forbidden result or harm. All criminal acts are defined in this manner. Spamming, spoofing and hacking to name but a few have not been defined in a criminal sense are not included in the statutes!

Many reported cyberspace crimes mirror traditional offences such as theft or fraud and they pose particular problems for detection, prosecution, and prevention. Several factors make this type of criminality difficult to address. Lawbreakers have now integrated complex technical

methods with traditional crimes and we have seen the emergence of creative new methods of committing criminal acts. These people use computers to cross national boundaries electronically, thus complicating investigations. Moreover, the evidence of these crimes is neither physical nor human but, if it exists, is little more than electronic impulses and programming codes. To make matters worse, computer crime is sometimes difficult for to comprehend and to accept as a major problem with a local impact.

A gargantuan IT security industry has grown up around the emergence of cyberspace; but ask most IT security professionals what they are protecting against and the notion of "crime" rarely enters the argument. Even fewer are able to define "crime" in any meaningful way and relate it to why they implement costly security procedures in the first place. A crime is not what someone wants it to be, as seems to be suggested by many writers on the subject of security and who use words like sabotage and hacking when no such offences exist in law. Crime, we have said, has a particular definition: an act of disobedience to the law forbidden under pain of punishment. This differs markedly from security. Like security, the aim of the criminal law is to protect individuals and property from harm and it dose so in two ways: before the event by attempting to deter the proscribed act; and after the event by providing sanctions against those properly convicted of the act. The notion of crime plays no physical part whatsoever in preventing a proscribed act, as security does.

And law enforcement fares little better, as it seems that most security managers are unaware of the manner in which evidence in criminal proceedings is demanded. The correct formulation and implementation of Cyberspace crime prevention which is a function of security, will help businesses to meet the investigatory and evidential requirements of these two acts by enabling managers to minimize the likelihood of a computer not "operating properly" or being "out of operation" by demonstrating "correct functioning". A consequence of the increased emphasis on security has been that the IT security staff is often viewed by management as investigators of a variety of security breaches, misuse of IT resources, email abuse, and network attacks, both internal or external. The evidence available shows that rarely do IT security staffs have any knowledge of, or have received any training in, investigation; they are therefore dangerously ill-prepared for the task of properly conducting a thorough, professional, and impartial investigation. In addition, they are unable properly to identify, handle, and examine evidence that resides in digital or other format. Finally, they are ignorant of the stress factors, both personal and professional, which often accompany the role of investigator.

Extending the rule of law into cyberspace is a critical step in the creation of a trustworthy environment for people and businesses and the growing danger from cyberspace crime is beginning to claim attention in national capitals. In most countries, however, there is a substantial risk that existing laws are unenforceable against such acts. This lack of sound cyberlaw means that, today, businesses and governments must rely primarily on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Technical security solutions are not sufficient to make cyberspace a safe place. Countries where legal protection is inadequate will become less able to compete in the new economy. Accordingly, national governments should examine their current statutes to

determine whether their laws are sufficiently robust, scaleable and flexible to combat cyber crimes. Often forgotten is the onus business directors and managers have in providing secure environments, often without knowing it; legislative, regulative and compliance issues are growing in importance!

It is said that society and its institutions have already have fallen behind information age criminals; at this point, we must now ask the question not whether we can catch up but whether they can keep the gap from widening. Beyond the technology of Cyberspace there has been a deep and worrying lack of research in this area. It is now time for researchers to explore, analyse and explain the problems in far greater detail that hitherto. We need to understand the origins, methods, and motivations of this growing criminal group. Decision-makers in government, the legal profession and law enforcement must react to this emerging body of knowledge. We must seek to develop policies, methods, and regulations to define crime in Cyberspace, to detect crime when perpetrated, to properly and thoroughly investigate criminal activity in Cyberspace and to prosecute those responsible.

Cyberspace has given us a new age filled with the potential for good. Cyberspace has given the criminal new opportunity. The approach to cyberspace law enforcement must change if new ways are to be found to keep the drawbacks from overshadowing the great promise of the information age. The need for sound and comprehensive crime prevention and detection management in business organizations remains as strong as ever. With almost all organizations now embarked on the development of a new generation of Cyberspace technologies it is necessary to ensure that this new environment offers an appropriate level of protection against criminal activity that is scaleable, flexible and manageable. In turn this should mean a firm policy on the investigation and prosecution of offenders. It rarely, if ever, does. It is time to review and assess the current thinking about what is called computer crime and criminal acts as they relate to crime prevention and its management in the information age. To do this we need a methodological approach onto which we can map current ideas and set them against validated approaches to assessing the concepts illuminated by writers and thinkers, theorists and practitioners and against the abstract and the factual.