Originally Published in the Book "Hacked Attacked & Abused" , By Peter Lilley, Published by Kogan Page

PREFACE: WIRED FOR CRIME

"I never think of the future. It comes soon enough"
-Albert Einstein

"I'm sorry Dave, I can't let you do that"
-HAL, the seemingly all knowing computer of "2001: A Space Odyssey"

You can phone virtually any country from a mobile phone as small as a packet of cigarettes. That mobile phone can receive and send endless text messages to another phone, or a computer. Most probably if you use text messaging regularly you will communicate in a shorthand language that is (thankfully) indecipherable by your parents. You can receive news, stock prices or sports scores on the same phone. If you want to convert one currency to another or carry out any other mathematical calculation the same phone will no doubt be able to do it for you.

Access your computer, log onto the Internet and the whole world is yours. You can bank online- you can even open your account on-line. That account no longer has to be in your native country, let alone the bank on the corner of your home town. You can choose and order your groceries online. You can trade stocks. You can book flights, hotels, taxis and anything else you need for your travel plans. You can search for old friends, or advertise for new friends. You can access and download newspapers, books, film scripts, research papers and millions of other documents. You can consult telephone directories, company filings, university student registers and an almost unimaginable number of other public (and some not so public) records. You can –even after Napster – download your favorite musical track. And you can get a palmtop computer, like I have, that measures 18 centimeters by 10 centimeters with a long battery life that can do all of these things from anywhere on the planet.

You can work from home and communicate with anyone, anywhere by e-mail with a click of a mouse. You can give a telephone number in Switzerland but when it is dialed the caller is seamlessly transferred to a telephone thousands of miles away. You can even have a phone number in virtually any country of the world which when answered records a message and sends it as a file to be accessed by e-mail. When you pay for goods you are now probably more likely to do it with a piece of plastic that is validated and processed electronically – standing, for example, in Singapore but taking money electronically from your account in Spain. And if you should need cash, you can get it 24/7 from an electronic machine in a wall, any wall, anywhere in the world.

We now live, work and play in a digital age. In computer terms, Digital refers to any system that is based on discontinuous data or events. Computers, for example, are digital because they can only distinguish between on and off, positive or non-positive or 1 and zero. All digital data must be encoded as a series of ones and zeroes. Each of these state digits is referred to as a bit –and when strung together in a format that a computer can address individually as a group is a byte. Digital has entered our vocabulary with a vengeance in the twenty first century: every form of media has been digitally remixed or remastered; we have digital cameras, digital photographs, digital libraries, personal digital assistants, digital television, digital images, digital scanners; websites abound with "digital" as a prefix or suffix – digitalwomen, digitalmedia, digitalproducer, digitaljournalist, digitalaudio and somewhat obviously, digitalsex. Ironically much of the digital age relies on conversion from analogue to digital and vice versa: modems convert digital information to analogue signals for phone line transmission (and the other way round for incoming data); Compact Discs store analogue forms (music) in a digital form, but when they are played the CD player reconverts the digital information back into analogue form so that we can listen to it.

We live in world that has changed beyond recognition in the last ten years: it is now almost possible to live your entire life online or through technology. Increasingly we have been sold this vision: not only individuals, but the business world too. Manufacturing companies suddenly turned themselves into cutting edge high technology concerns; analysts and financial institutions put complete faith in technology investments; small companies were told that unless they had an Internet and e-commerce plan they were doomed. Dot coms were the future – and everything else was junked, until of course the dot coms themselves became junk.

But just like real life, the high tech existence came with risks, and a dark shadowy side. Not that it was envisaged in the early days of this brave new world or appreciated that such a dark side would exist: but exist it does. The Internet simultaneously liberates and imprisons: Pornography, pedophilia, hate sites, grudge sites, terrorist information – you can find it all, in glorious detail on the Internet. Want to rob a bank? Want to learn how to build a bomb? Want to rubbish a company or person? Want to stalk? You can do all of these things on-line. What has become obvious is that the tremendous advances and opportunities that technology has delivered have simultaneously opened up a Pandora's box of possibilities for darker, sometimes evil, deeds. Terrorists, organized criminals, fraudsters, money launderers have all grasped the advantages offered by the Internet and other related technologies. Hackers, Crackers, Virus creators have all tried – and succeeded – in subverting the on-line environment. We have been sold the lie that technology provides us a safe, sterile, forward-looking environment: whereas the simple truth is that all of the risks and dangers inherent in normal life are magnified on-line and in high technology. Magnified, but to a large extent, ignored. It appears increasingly that we are unaware of the dangerous roads we are traveling along.

Cyberspace is not a real place (or is it?). Some of us probably think of cyberspace as the images that appear on screen when we participate in a playstation game: when we drive an imaginary (but strangely realistic) rally car, or kill an opponent in a war game, or score a goal in soccer. Cyberspace may not be real, but it is not false either: very real events happen in cyberspace. Many of our personal details are there or can be accessed through there; many of our conversations (whether they be via phone, mobile phone, e-mail or fax) pass through there; the actions we take in cyberspace (what websites we access; what calls we make; what programmes we watch) can be recorded and monitored.

This book does not seek to present an alarmist vision of the digital age. But simultaneously neither does it attempt to airbrush out the grave risks and dangers that are ever-present in this brave new environment. This is not a technical book – in that it does not reproduce lines of software code that will magically solve all of your digital security problems. What this book does attempt to do is describe and analyze the risks

inherent in the sustained and continuous reliance on technology. Primarily this is viewed from a business focus, but as ultimately we are all customers, the perspective cannot be a narrow one.

It continually strikes me that we do not realize the fault lines that we tread on each day when entrusting our communications, personal details, confidential material or whatever else to technology. In early 2001 the FBI warned that a successful hacker attack against the United States banking and financial system could cripple the country within three days – Alan B Carroll who supervises the analysis and warning component at the FBI's National Infrastructure Protection Center observed that "We cannot afford to let our dependence on automation become our Achilles heel. Our challenge is to button up the holes in our critical infrastructure, and believe me, there are holes" The FBI has identified eight critical infrastructures that are heavily dependent on technology, and thus prime targets for attack. These are:

- Utilities
- Oil and gas
- Telecommunications
- Transportation
- Banking and Finance
- Water
- Emergency services
- Government operations

At the opposite end of the panic spectrum are the merchants of doom who continually and repeatedly bang the drum warning of an electronic Pearl Harbor. These observers warn that because twenty first century technology offers an infinite number of points of attack, the possibilities for future wars or individual battles lie in the digital domain. They write (endlessly) about attacks on mobile phone networks, cash dispenser systems and similar global structures. I used to have some sympathy with their views, but after the horrendous events of 11 September 2001 I have severe and abiding doubts about these predictions of so called doom. In the end, who cares if the world's ATM networks crash? Is it the apocalypse if your mobile phone fails to function?

Certainly interference or sabotage of such safety critical networks such as air traffic control would lead to dire consequences. Yet the indescribably tragic events of 11 September 2001 do not suggest to me that the digital world is the new global battleground: rather that our reliance on technology actually dulled our responses and left us open to attack. The suicide pilots basically stole four planes and then (in three cases) converted them into highly efficient flying bombs, ramming them into key physical structures populated by thousands of innocent people. The hijackers (in the actual outrage) made little use of technology per se, but even more alarmingly all of the technological systems that were supposed to warn against such attacks failed completely. Moreover the background support of intelligence collection by electronic methods was also shown to be utterly inefficient. None of this is to underestimate the technology that was almost certainly used to achieve effective, coded communication between the terrorists – or the computer wizardry employed in the subsequent military attacks by the United States or their allies.

Perhaps the safety controls that were in place did not react, or swing into action quickly enough, because there was no prior knowledge or expectation of what occurred. Blame the hardware and software systems that were supposed to protect us, then. Well, no…all technology ultimately is human created, programmed and maintained. In the marvelous, ground breaking film "2001: A Space Odyssey" Stanley Kubrick brought to life, so to speak, HAL. This "Heuristically programmed Algoritmic computer" was supposed to be as near to an artificially created intelligent machine as possible: so much so that HAL ultimately thought that it (or should that be he?) knew better than the human occupants of the space ship and promptly cut off their life support systems. However clever HAL thought it was, and independent of humans ultimately a human could terminate its existence by cutting off HAL's critical functions.

Similarly, all technology that we utilize today – however advanced – is human dependant. We cannot blame "the technology": because we created that technology. In business the convoluted (but no doubt necessary) procedure to design and install a new system begins with the user specifying its needs and requirements, and should end with an ongoing review of whether those needs have been met by what has been delivered. Trap doors exist in systems because the designers and/or programmers left them there; computers may "be hacked" but the hacking is done by (probably) a male

Caucasian youth aged under twenty. This morning I phoned up my bank to make a very general query about my account, only to be informed (on three different occasions) that the system was down – which is a description not a reason. For the bank's system to be down, somewhere back along the line was a human error(s).

More prosaically, and closer to home one e-mail that I recently received – from an e-mail service that (fortunately) I use infrequently stated that:

Dear Client
We are currently performing unscheduled maintenance to your e-mail server due to unforeseen circumstances and the service is temporarily unavailable. Email residing on the email server has been lost and will be unrecoverable. Your email service will resume again shortly. Please try assessing again later. We apologize for the inconvenience caused.

In other words, if you held all of your present and past correspondence in email form of this server, you had just lost all of it forever, never to be recovered. But most email users rely on this communication channel, until they receive a message like the one above.

This same provider warned customers a few months earlier that their web hosting system was struggling to operate because of sustained denial of service attacks which were crippling the entire setup, making it impossible for websites to be accessed.

Even more surreal was the un-solicited e-mail that I recently received from a pornography website. Never mind that my e-mail address had obviously been obtained from my website via a "sniffer" program. What amazed me was not the financial offer made to me, but the problems that had been previously experienced:

> Site XXX raises the Bar Again and Increases Payouts
>
> Site XXX reduced payouts in response to Webmaster fraud a few months ago. Now with vastly improved fraud detection technology, Site XXX is pleased to

announce that payouts have once again been raised above all other programs available to adult webmasters

Pornography and gambling have increasingly become the two business areas that are perceived as being able to generate profits via the Internet. Whilst many observers would argue that these two sectors are prime representations of the dark side of technology, or the effects of it, both pornography peddlers and on line gambling sites are vulnerable and frequent targets of criminal attacks.

On-line gambling is surely one of the most interesting business sectors of the Internet: a sector that is solely based on money and could already be worth $2billion. The Internet is populated by thousands – if not millions – on on-line gambling sites, many ostensibly operating from obscure offshore locations. On reflection, such sites are an obvious target for fraudsters and hackers. It is now becoming evident that hackers are regularly obtaining large sums from these sites. In August 2001, a Canadian company that handles online casino games confirmed that a hacker had corrupted one of its games so that players could not lose: so for a few hours gamblers on the site obviously thought that they had accessed their idea of heaven. In that short time period 140 gamblers won a total of $1.9 million. Then to compound the situation, in some instances, the intruders had blackmailed the on-line operators: demanding large sums from them to "guarantee" that further such attacks would not recur. Whilst never confirmed in the public domain by relevant operators, it is widely suspected that some attacks and subsequent extortion requests originate from Eastern European organized crime groups. Like much hacker activity, attacks on gambling sites take a variety of forms: there have been various denial of service outrages which disable the relevant site. Such denial of service attacks, if timed to coincide with major sporting events can have very effectively deprive the operators of massive sums of bets. These incidents happened at real sites: there have also been various fraudulent gambling web sites created. Such sites give the appearance of being a legitimate betting forum but in fact are nothing more than a scam. Keen punters fill in their credit card details so that they can place bets. These customers will never see any winnings but will, when they receive their credit card bills, realize that the criminals behind the site have utilized their credit card as much as possible.

Even more frighteningly, the forward march of new technology is already impacting on our personal lives in sinister and previously unimagined ways. As an example it is now very easy to buy software that records all activity on a computer. Such software can be used, for example, by employers to monitor their workers internet and computer activity. It could also be utilized by a company to spy on a competitor or rival. These software programs can also be used in the domestic environment: the advertising material actively promotes such usage to monitor the computer activity of partners and children while you are absent. There have already been examples (and court cases) where an estranged partner has hacked into the computer of the other partner and installed software which then e-mails him or her (without the user's knowledge) details of all key strokes, web surfing and internet communication. You don't have to be paranoid about all of this, but it certainly helps.

And strange, unpredictable events occur in the digital age: one survey in the United States conducted by Cyberatlas in early 2001 showed that 8% of US Adults and 12% of US Teens use the Internet for religious or spiritual experiences. In Brisbane, Australia in October 2001 a man was jailed for the seemingly obscure crime of hacking into council computers that control sewage. He succeeded in, amongst other things, getting a sewage pumping station to overflow thousands of litres of "material" together with pumping raw sewage into public waterways. In all he was found guilty of thirty charges including computer hacking, theft and environmental vandalism. His motive was pre revenge against his former employer (the installer of the sewage system) and the council which had turned down his job application. An even darker side of web activity are the claims (which have surfaced in relation to a number of separate events) that the Internet has been used to facilitate murder. Ofir Rachum was a 16-year-old Israeli boy who apparently established an online relationship with an older female American tourist who was staying in Jerusalem. The relationship moved from chat rooms to e-mail to telephone conversations. After meeting once in Jerusalem Rachum met his online friend again in January 2001. Whatever the girl's original intentions, it appears that she was persuaded by the Palestinian Tanzim group (armed militia) to lead Rachum to them. He was shot 15 times. His body was found in the boot of a car on the outskirts of the Palestinian town of Ramallah.

This book seeks to provide an overview and evaluation of crime, fraud and risk in the digital age by exploring how we got where we are now, where we are going and what risks we face on this journey. To chart this journey we begin by reminiscing about the good old days, when computers were mainframes and mobile phones were the province of science fiction. From there we travel to the digital age of the twenty first century, looking at key milestones en route: such as the fact that in 1995 each American used annual average of 731 pounds of paper, more than double the amount used in the 1980s – so much, then for the paperless society that technology was going to deliver. After considering just how far and fast technology has developed and impacted on our personal and business lives, we then turn to evaluate just how and why our considerations of computer and electronic crime have always been underestimated and subject to fatal ignorance. This ignorance has been transmitted into the legal and investigative process, where even now the concept of a global technology driven economy, with all the risks inherent in that is not sufficiently (if at all) embedded in the legal system.

Part two concentrates on the various forms of attack that occur on technological systems and programs by together with the use of technology to facilitate criminal activities such as money laundering. And what a mixed bunch of attacks and attackers we face in the digital age: from hackers, self-inflicted errors, money launderers and virus writers to name but three.

The Internet itself forms the basis of Part three of "Hacked, Attacked and Abused". In 1993 Bruce Sterling saw the Internet as "a true, modern, functioning anarchy" – a borderless community with very few, if any, rules and regulations. So the scam website that an investor has just lost money to may quote an address in New York, but in fact the crooks behind it are in Russia using a first stage bank account in the Caribbean. Multi jurisdictional crime such as this is difficult to prevent, investigate and prosecute; if only because of the immense problems encountered where different country laws, official bodies and – it must be said – turf guardianship abound. The Internet is truly global, but there exists no international body to police, regulate and control it.

Whilst I am skeptical of the claims of an impending electronic Pearl Harbor, in Part four consideration is given to the claims made that some countries are already using technology extensively to "attack" other nations. Moreover, and just as critical an issue, if countries are doing it, why can't businesses utilize identical techniques to grab competitive advantage from their rivals.

One of the key issues raised by the digital age is the loss of privacy that is implicit in many of the transactions conducted on the internet, records held on computer or conversations conducted across the ether. In Part five "Privacy Lost" an attempt is undertaken to quantify what information about us (as users, customers, subjects) is collected and stored. How is this information then utilized – and at what stage may that usage become unethical?

If by that stage of this book you have not become too distressed or despondent then Part six describes what practical steps technology users can take to manage and minimize the risks presented by electronic/digital crime and fraud.

Whether the digital age ultimately brings on such is gloom open to question, but I would not necessarily place any great reliance on a "security" product available in the United States. This is a gargoyle which is placed next to your computer and wards off modern day evils such as viruses, hackers and system errors. Just one version of such a security device has sold over 100,000 units- which either means that this number of people have computers wide open to attack, or the rest of us need a gargoyle immediately to protect us as these 100,000 wise users already have.