

COMPUTER CRIME!

What is it, who does it and why? Al Baron talks to author Buck Bloombecker about a book which explodes the myths and exposes the true cost.

Could you begin by describing *Spectacular Computer Crimes* for us?

My book summarises the work at the National Centre for Computer Crime Data in a way that illustrates how computer crime has become a problem affecting all of us. The standard view of computer crime is that hackers are the only criminals and the victims are all big corporations who can afford the loss. But that point of view is an invitation to bad security.

A company which only worries about hackers isn't going to worry about malicious or even ignorant people who spread viruses who don't happen to be hackers. There are many employees, ex-employees, even conference delegates who are involved in computer crimes that cost half a billion in the US and £1 million a year here in the U.K.

It's not a lot though, really is it?

I don't know how to relate to numbers that big. A reporter once said that the cost of traffic tickets in the United States was probably much greater than the cost of computer crime.

But the seriousness of computer crime is certainly enough to justify legislative attention, and for a computer user to say: "I'm losing money here and could justify spending some money on computer security."

For an individual PC user, if you haven't worried about computer viruses yet then it's none too soon to start – particularly if you're using bulletin boards or if you're getting hold of a lot of software.

Wouldn't you like to see standards adopted?

Most American computer crime laws already say if you damage a computer system or any part of it, it's a crime.

With intent?

Yes, with knowledge. If you know what you're doing and you do damage to the system – that is enough. You can say that you didn't want to cause anyone any harm. Robert Morrison didn't want to cause anyone any harm and said: "Well it's too bad 6,000 computers were interfered with by my program." But there's a difference between saying, "I didn't know I had a virus" and "I had no idea what my program would do". The first is easy to believe but the second is a more questionable area.

What did he get?

Fined \$10,000 and with 200 hours community service.

That's not a lot either is it?

Oh, we have to fight against the implication that you won't be seriously punished if you're convicted of a computer crime.

Tell us about some of the crimes in your book.

The first chapter is about a man called Schneider: Jerry Schneider, who ripped off his local telecommunications company in the San Francisco area when a kid

in 1971 and who is now an international banker. I use Schneider to demonstrate some of the myths of computer crime and to contrast that with reality. The myth is that Schneider went from a computer criminal to a computer security consultant, and the presumption is that he is fabulously wealthy as a result. In reality he never made a dime as a computer security consultant.

In the course of my research I found that Schneider claimed he'd worked for IBM, Honeywell, and AT&T. I called one of the consultants who had asked Schneider if he had been a consultant for all these people and he had replied "yes, by all means". But when asked if they'd paid him Schneider had said "no"! My colleague felt he'd used the term "consultant" rather loosely.

What motivates a computer criminal, greed?

There are several types. The 'Sandbox' type is someone who just likes to play with computers – your typical hacker, in it because it's fun. But there are people who are in what I call the "land of opportunity". They will say "the trust fund was just sitting there!" A lot of employees commit computer crimes not because of the challenge but because of the lack of challenge.

Then we have the 'Battle Zone'. In my book there's an example of a fella who destroyed over 100,000 records. He was annoyed with his company because they wouldn't let him engage in a tax protest. The global



•Buck Bloombecker: fighting computer crime with information.



version of this is the 'Soap Box' instead of the 'Battle Zone', someone who commits a computer crime to make a political statement. One example is a woman who destroyed a computer she believed was going to be used for first strike attacks on the Soviet Union.

How did she destroy it?

Physically! She took a crowbar and whacked away at it.

I'm surprised that is classed as a computer crime!

I admit that not everyone does, but my point is what is computer crime? We can define anything we want as long as we have a reason for doing it, and I think the need to define computer crime is to protect computer systems. We are investing more and more time and money in computer systems, from individual PCs to enormous interconnected networks.

If we had a lot of people going after computers because they want to destroy them for political reasons then that is important data for security professionals.

Who's the worst computer criminal in your opinion?

I take a certain perverse pleasure in saying that of all the criminals I have analysed none of them were sufficiently evil in motivation or devastating in their effect to really qualify. I think the ones caught so far have been typical human beings, motivated by greed or malice.

Oliver North, is he a computer criminal?

Well, I say his computer crime was trying to steal history. He didn't succeed but I certainly worry about a Government official using computers in an attempt to cover up his misdoings. Particularly when it is part of this preposterous theory of deniability: where a President thinks he has the right to set things up so that when his crimes are discovered he can pretend that he didn't do them. Of all the people in my book he is the one I'm most annoyed with.

What about computer crime myths. 'The salami technique' for instance where the criminal tops up all the half cents on the payroll and then has them made out to his pay cheque at the end of the month. That was actually used in a Richard Pryor Film.

There may have been a few cases, but like the alligators in the New York sewers it is kind of a myth.

What other myths are there?

I like to go after the myth that the victim is a large, rich computer corporation which can afford the loss many times over. Another one is that all computer criminals are computer experts. I point out how someone who knew nothing about computers set up a two level fraud system.

At the first level he stole money from 1,600 computer users by saying: "Let me rent your spare computer time and pay you per hour while you use my software/hardware to make automated phone calls to people". That was a simple scheme because he just didn't pay people and collected all their deposits of \$525. The devious part was the purpose for which these people were using their computers – to make calls advertising a trivia contest that was totally bogus, there was no contest, no first prize, no trip to Atlanta, nothing. With 1,600 people using their computers to make hundreds of calls, we are talking tens even hundreds of thousands of people, victimised at least to the extent of having to listen to this fraudulent scam, and in many cases being taken in and sending in money.

These people were as sophisticated as your readers, yet they fell for it. Partly because the guy had 'Cow Lists' – lists of people who had been victimised or milked before and who he felt could be victimised again.

Consumers of computer goods and services have got a raw deal because the consumer protection movement hasn't the energy to take care of them and the industry has not matured enough to set up much in the way of consumer protection. Stories of lack of customer support are legendary: calling the support number for three days and not getting a call back or getting unreadable documentation.

I spoke to a member of the City of London Police who said computer crime is virtually non-existent and hackers are regarded simply as a pest. Is it a myth about hackers breaking into banks?

75 per cent of computer crimes in the States involve a theft in which the computer plays a significant role, and even more cases involve theft of communication services as well. The other 25 per cent of computer crime in the US involves hackers of one form or another, so to say that hacking is not extensive is certainly inaccurate.

Computer crime is like an environmental issue. Crimes committed now are indications of weaknesses in our security systems, in the way computers are produced, or in the provision of computer services. If we heed the warnings we can develop effective strategies before the situation gets out of control.

Computers aren't going to destroy the environment, but what could they destroy? Freedom?

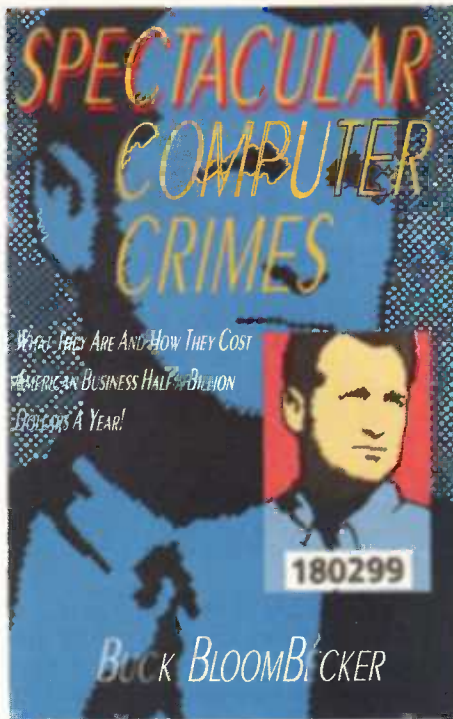
Look at the systems that rely on computers – nuclear reactors, network control systems, traffic systems, hospital life support systems – inadequate security in areas like these can be the key to a really dramatic disaster. One of the greatest computer-politics triumphs of recent times was the block we put on Star Wars in the United States. The argument that dampened the enthusiasm for Star Wars was the poor technological feasibility of the system. An enthusiastic President putting up an untested system which could have increased the likelihood of nuclear war... it would have been a disaster.

We have this myth that computers are a totally positive, totally harmless technology. As if none of the by-products of capitalist industrialism that have affected other environmental issues are going to arise from the increased use of computers. I think that's foolish. Without proper attention to safety, anything that has that much impact on our society must be watched carefully.

But you posed the other side of the question, whether computers threaten our freedom.

I was thinking specifically of databases. Can we deal with the Big Brother aspect and the flow of information? What are your views on companies selling mailing lists and personal data on people?

I think the concept is worrying. Having interacted with a number of government agencies and having had first hand experience of the US Freedom of Information Act (and knowing how little help that is to the individual), I feel insecure. I am troubled by the knowledge that I don't know what government agencies may know about

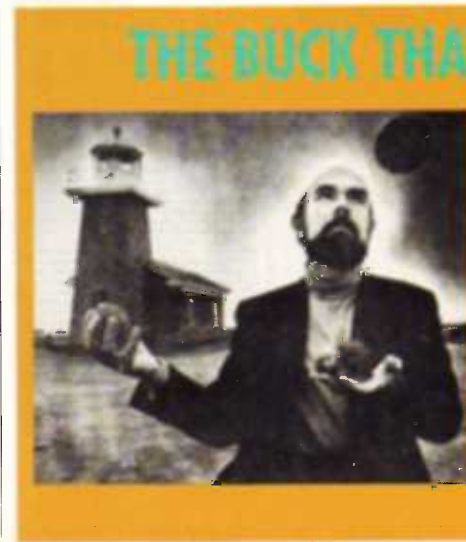


me, may share about me and what consequences for my professional career that data may have. Anyone who thinks about the problems of information and the use to which it is put has to share those fears.

I am comforted by the inefficiencies of the American Government in terms of making use of all this information. If the people who are pledged to defend our liberty are no more technologically sophisticated than Richard Nixon or Oliver North, who thought he could erase documents by pressing the delete button, our privacy is safe because they're too stupid to invade it.

There are a lot of people as dumb as those two and the big business of the future will be picking out the garbage. The computer revolution has increased the volume of garbage to the point where that may be our best defence. It's the way I protect my office; there are 35 boxes of filing that need to be done on top of the filing cabinet. It would take so long for anybody to find anything of value they would just look at it and say: "Lets find somebody who is organised, he'd be a much better target."

However, I've just read about hospitals getting certain services in return for making patients' databases available to data processing agencies, so that the agencies could send letters to everyone who was pregnant, or who had just turned 18, or whatever. I think that this is abominable.



Do we need laws to protect us from Government?

I'm not sure the law would be an effective way round that problem. We passed the Privacy Act in 1974. I researched the extent to which Americans believed their privacy is protected more from computers now than it used to be, and the number of people saying "no our privacy is less protected" is increasing.

Are they right, is their privacy less protected?

I think more correct information is being collected all the time although I'm not sure how much of it is being used.

My prejudice as a lawyer is that action against the Government for violation of privacy might serve us better than either regulatory schemes, like the Data Protection Act here, or the Privacy Act in the US. The US act doesn't seem to work even when enforced by two fisted regulators.

Let's talk about viruses. Virus vandals – do people create viruses and hold governments to ransom?

I haven't come across any instances yet. In fact one of the things that puzzles me is how so much development has gone into viruses without anyone figuring out how to gain from them. I guess the closest we've come was that guy who was sending thousands of AIDS information disks around and supposedly following up with virus threats and demands for money. Apparently he turned out to be deranged and his disks were not dangerous.

Could even talking about this give people ideas?

I don't worry too much about putting ideas into people's heads, I worry more about not putting balancing ideas in other peoples heads. Most genuinely concerned people would be inclined to side with me. Incidentally, I'm very curious about the withdrawal of *The Hackers Handbook*.

I don't understand the reason for withdrawing it, or for threatening prosecution if it wasn't withdrawn. It would be hard for me to imagine that happening in the United States. If they did they'd have to take all the books on fraud investigation off the shelves and you can't teach how to investigate fraud without describing fraud. If the only difference between my book and *The Hackers Handbook* is tone then I'm nervous – because tone is in the eye of the beholder.

I used to use a speech called 'Computer Crime – the Career of the Future', but people came away saying "You seem to be encouraging computer crime". So without changing the context my next speech was called 'Why I'm not a Computer Criminal'. I made fun of Stan Rifkin, he converted \$10.2 million into diamonds and then didn't know what to do with them! By the time he was arrested he told the police "I've been practising for you to question me". This is not the glamorous, computer criminal image the media sometimes portrays. ■

● *Buck Bloombecker's Spectacular Computer Crimes, is available from Charles Letts and Co Ltd, Diary House, Borough Road, London SE1 1DW. Price £18.95*