Copyright © 2007 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 Vol 1 (2): 249–251

Book Review of Cybercrime – The Reality of the Threat

Nicholas Chantler[1]
Queensland University of Technology, Australia

Nigel Phair, Cybercrime: The Reality of the Threat, August 2, 2007, BookSurge Publishing, 190 pages. ISBN: 978-0980342109

If you're looking for introductory text on what cyber crime is, then this is the one! But don't expect and in-depth academic text. This self-published book is very much a book for the operational practitioner. An easy to read text that provides a broad overview relating to Federal Agent Nigel Phair’s experience whilst working at the Australian High Tech Crime Centre in Canberra and as a member of the Australian Federal Police. Some comments may seem to appear rather glib, along with several assumptions, but don't be put off; the book has merit and Phair provides a good insight for the newcomer wishing to learn about the domain of cyber crime.

The introduction, I presume in an effort to allay our fears, states "The Internet is not of the Wild West, as was once portrayed in American Western movies. It is just another public place and Internet users need to use real-world sensibilities when operating in the online environment." Phew, thank goodness for that! But his statement is quickly followed by a darker one of impending doom; "the communities trusting e-commerce activities, will slowly erode over time as personal users either become victims of online crime or know someone who has." He then briefly mentions ‘the profile of cyber crime criminals’ and how the hacking the counterculture has completely changed into well-organized and hierarchical groups of criminal syndicates that have realized there is substantial money to be made by criminal activity online. A geographical overview of the cyber crime elements are presented as the only real risk from Eastern Europe, Asia and West Africa. This is just too brief. His Eastern European perspective focuses only on the Russian Mafia and one incident involving a Romanian National. Asia, primarily relates to issues in China, although Singapore and Korea do get a mention. West Africa, primarily focuses on Nigeria and Kenya; with the Nigerian activity relating to the infamous "Nigerian letters."

The rest of the book addresses the cyber crime activities under the broad headings of:

- Unwanted Software;
- Identity Crime;
- Phishing;

[1] Lecturer, Room: X517 (Gardens Point Campus) Queensland University of Technology, Brisbane, Australia Email: a.chantler@qut.edu.au

- Critical Infrastructure Protection;
- Intellectual Property;
- Communications;
- Terrorism; and
- Enforcement.

Under the heading "Unwanted Software" hacking activities are mentioned. Not only are they apparent from outside an organization, but also from the inside. This is where 'spyware', a software program, collects information about the user without the consent of the user and sends it to third-party without the user's permission or knowledge. Phair explains 'spyware', 'adware' and 'cookies'. He considers the impact of this software, and explains what trojans, key loggers, rootkits, viruses, ransom ware, worms, botnets, denial of service (dos), extortion and spam, all mean in the cyber crime arena.

Then 'Identity Crime' is explained from the perspective of phishing for information; proof of identity; how financial data is lost; how identities are sold; and, the age old problem of correctly identifying Internet users. The section under 'Phishing' considers the origins, along with the tools and techniques, of specific cyber-criminal activities such as pharming, severe phishing, vishing and authentication. The size of this problem is also presented which leaves the reader with the opinion that this aspect alone is only 'the tip of the iceberg' of cyber crime. 'Money Laundering' has been around for a long time. But since the further development of technology, there seems to be so many more ways to be able to launder money. Phair considers what one does with the proceeds of crime. He explains alternative remittance systems (such as 'hawallahs'), and the financing of terrorists.

The National Information Infrastructure (NII) is something that we all rely on; but, I suspect we all tend to take for granted. It is our life-blood for telecommunications and computer networks – never mind what's connected to it (banks, stock market etc.). Nigel Phair reminds us that 'Critical Infrastructure Protection' is paramount in guarding against the collapse of the NII. This involves consideration of the risks to; and also from, the Internet itself. There are those perceived foreign threats; environmental factors (fires, floods etc.); and, then there is SCADA (supervisory control and data acquisition). SCADA involves all those simple electronic controlled things, sluice gates, sewage control, weather stations, security cameras, traffic controls, gates, etc. All these things seem innocuous until connected to the internet for communication. The trouble is when an unauthorized user gets access and starts to control SCADA devices, things can go wrong. Nigel Phair mentions the unique 'sewage-case' in Queensland.

'Intellectual property' focuses on software piracy and the sharing of files through some of the well-known peer-to-peer systems such as napster, grokster, and kazaa. It's an area of concern that also addresses the difficulty in identifying users; and the issues of jurisdiction. The continued technical growth in telecommunications and the concerns it raises are presented in the 'Communications' section. Don't be too concerned with the 'technocrat verbology' that follows. Nigel presents in plain-English an overview of the technology with some of the weaknesses, the risks and the threats. These include wireless devices, VoIP (voice-over-internet protocol) - such as Skype and Google-talk, third generation phone systems, issues with caller ID, clipping, v-bombing, sim boxing, internet dumping, PABX hacking, phoneline scanning, voicemail, cloning, Bluetooth, and RFID. He also relates these technologies to issues of privacy.

The final two sections consider 'Terrorism' and 'Enforcement'. Here Nigel Phair explains how terrorists capitalize on the anonymous nature of communications on the internet. He also mentions information warfare (considered of military importance) and the distributed denial of service (ddos) attacks. Politically motivated groups seem to be associated with the cyber terrorist activities and Phair gives good reasons why. There are many aspects that cyber criminals use which are also available to the cyber terrorist. In the final section 'Enforcement', Nigel presents some recommendations and perspectives relating to the law enforcement response, the role of ISPs, and civil prosecution. He reminds us that cyber crime is a global jurisdiction issue; and, he suggests that perhaps there should be an economic consideration in combating crime; allocating resources to make punishment more severe or more certain; and, consider creating severe fines as opposed to imprisonment.

Now the book's conclusion may seem rather abrupt and pithy – it is very brief – with statements like "information technology has transformed the way we live in a very short time." But it does make the point that his main message is "the requirement for swift and coordinated international action to keep Cyber criminals in check." I must say that I was surprised and disappointed to find virtually no information about credit card fraud and the "carders", ATMs (automatic teller machines), hardware hacks and forged documents; along with a greater scope of explanation of other types of "rogue code" such as time bombs, growths, rabbits and tumors. An issue in dealing with any topics such as this, is the dynamic nature of the changes within ICT (information communications technology). The cyber crime environment is no different; consequently, it is very likely that by the time you have read this book a new way of committing a cyber crime is being developed. Don't expect a perfect document, some of the statements are without any references and you will find typos; never-the-less it is a very good beginners guide.