

Cybercrime: The Reality of the Threat

By Nigel Phair

Canberra, Australia: E-Security Publishing, 2007, ISBN 978-0-9803421-0-9

Price \$19.99, pp. 178

Reviewed by Michelle Hodges

Suffolk University Law School

Journal of High Technology Law

“Internet technology has transformed the way we live in a very short time. The most notable feature of this phenomenon is the extraordinary rate at which it is developing . . . For the law biding this rate offers opportunities for improving the way in which society operates. For the criminal it offers even more ways in which to plunder society.”¹

Since the advent of the Internet and increased globalization, the ability for criminals to commit all acts of cyber crimes has increased. Cyber crime “is the fastest growing form of crime” and “It is also the most under-reported and the least prosecuted.”² This book focuses on the increased rate of cyber crime throughout the international community and attempts to draw attention to the vulnerabilities to which individuals are exposed while conducting activities through the Internet. In *Cybercrime: The Reality of the Threat*, the author provides a survey of all areas of cyber crime, from spyware and hacking, to identity theft and money laundering, as well as well known intellectual property violations. He explains that the cyber world is a “new frontier for a new type of criminal”³ who has an incredible mindset for technology and access to all areas of the Internet where he is able to conduct these crimes from anywhere in the world. This is all written from the eyes of a Federal Agent at the Australian High Tech

¹ NIGLE PHAIR, *CYBERCRIME: THE REALITY OF THE THREAT*, 178 (2007). (Federal Agent Nigel Phair is a Team Leader at the Australian High Tech Crime Centre. He has been a Police Officer with the Australian Federal Police for over 17 years and he is currently a Senior Fellow at the Centre for Transnational Crime Prevention at the University of Wollongong in Australia).

² PHAIR, *supra* note 1, at 5.

³ PHAIR, *supra* note 1, at 178.

Crime Centre, who has seen firsthand the results of these crimes for the average citizen, state governments and large corporations.

The author's thesis is that we must educate individuals "whether private citizens, small business operators, large organizations or governments, [that] we all have the responsibility to be vigilant and to take all reasonable precautions to protect ourselves."⁴ No one is one hundred percent safe from an attack of a cyber crime, but there are several precautions that individuals can do to protect themselves. Only when individuals and governments, the end users of these crimes, accept the fact that they are vulnerable when they do not take the necessary security precautions, will the frequency of cyber crimes throughout the international community diminish.

Phair lays out his book in eleven chapters and the first chapter is devoted to defining who cyber criminals are and where they come from. The subsequent eight chapters are strictly devoted to defining the various areas of cyber crimes, how they exist, what individuals do to perpetuate them and what he proposes governments and individuals should do to prevent their continued existence. He chooses examples and cases come not only from his native Australia, but many important and pivotal cases from the United States, the United Kingdom and the rest of the international community, in order to provide the reader with clear examples of how these cyber crimes are continually committed. In the first chapter, however, he makes a clear point that unless the increase of these cyber crimes are decreased, the individual user of the internet will lose trust in e-commerce activities as more and more people become cyber crime. Therefore, it's necessary that the end users take the necessary steps to protect themselves.

⁴ PHAIR, *supra* note 1, at 179.

For example, in Chapter three the author points out that the anonymity of the Internet enables the cyber criminal to act as a virtually unidentifiable person. Moreover, the location from where he operates is equally difficult to identify. Whether the cyber criminal is sending spyware, hacking into government data, doing spam runs, stealing identities or laundering money, his identity is still anonymous.⁵ Therefore, the author introduces a proposal of implementing technology that “can be used by individual users as well as small, medium and large organizations to correctly identify and authenticate Internet users” in order to combat e-commerce fraud.⁶ This technology is called the public key infrastructure (hereinafter “PKI”).⁷ This particular technology forms a type of cryptography and establishes two keys, one that is used to encrypt information and one that is used to decrypt.⁸ The technology encompasses both a private and a public key, the private kept by the user and the public is to be maintained in a location known to everyone. Through this system, people wishing to prove their identities are provided with a certificate issued by a authorized body, which includes similar levels of proof as a bank account or passport. When an Internet user publishes his or her public key and if other users are suspicious, they can check with the authorizing body to determine if this is a valid user, thus enabling the curious person to link the user on the Internet to the actual person that has been granted this certificate.⁹ Then, if the user wants to prove that he is in fact who he claims to be, he would encrypt a message using his private key, which would only be known to him. In turn, this message would be decrypted by anyone who

⁵ PHAIR, *supra* note 1, at 56.

⁶ PHAIR, *supra* note 1, at 56.

⁷ PHAIR, *supra* note 1, at 56.

⁸ PHAIR, *supra* note 1, at 56.

⁹ PHAIR, *supra* note 1, at 57.

has the sender's public key and accompanying certificate.¹⁰ The author claims that the "use of PKI would be a significant step toward reducing the substantial amount of criminal activity that is perpetrated via information technologies because users [have] a unique digital signature that cannot be forged."¹¹ This proposal, however, may face various objections, which the author points out. First, it would require an international standard by which all users of the Internet must abide. Consequently, some jurisdictions may not want to become a party to an international body that regulates Internet user identities, which may potentially cause conflicts with protections of privacy. Additionally, the author could have provided a more in-depth explanation of the likelihood of PKI effectiveness. It is clear, however, that there needs to be some way to counteract the lack of prosecutorial methods available due to the anonymity provided by the Internet.

Additionally, when it comes to the issue of Phishing, the author reiterates a theme throughout the book-end users must change their policies in order to protect themselves and their consumers. Phishing is defined by the U.S. Department of Justice as "the use of e-mails and websites-designed to look like e-mails and websites of well-known legitimate businesses, financial institutions and government agencies-in order to deceive internet users into disclosing their bank and financial information or other personal data."¹² Phair does not provide a concrete proposal for addressing Phishing as he did with the PKI proposal. He does, however, suggest that banking institutions must take the necessary responsibility and acknowledge their own lack of security as a core issue in order to

¹⁰ PHAIR, *supra* note 1, at 57.

¹¹ PHAIR, *supra* note 1, at 58.

¹² PHAIR, *supra* note 1, at 61; *see also* United States Department of Justice-*Special Report on Phishing*, available at: www.usdoj.gov/criminial/fraud/docs/Phishing.pdf. last visited Nov. 18, 2007.

combat Phishing, rather than just reimbursing their customers and not addressing the crime's existence.¹³

In Chapter six, the author addresses the security protection that is necessary for government infrastructure. Many countries take a particular interest in protecting their national information infrastructure (hereinafter "NII"), which are their "computerized control systems which support all critical infrastructures, particularly those heavily reliant on information and communications technology for their proper functioning."¹⁴ This infrastructure is highly susceptible to attack by hackers and possibly even terrorist organizations.¹⁵ The author notes that the United States has chosen to retain oversight of the main Internet backbone for an indefinite period of time in order to protect the NII. However, the international community has not received this decision very well because "other foreign governments are concerned with another country having the ultimate control of their communications and data infrastructure through control of the high level root servers."¹⁶ The author proposes that "individuals who own and operate NII businesses need to build a culture of security across all business units and conduct vulnerability and risk assessments in a transparent way."¹⁷ The author emphasizes the need for businesses to express to their employees that security must be a part of the business process in order that employees understand the risks involved in cyber crimes as well as how these crimes could seriously adversely affect their organizations.¹⁸

¹³ PHAIR, *supra* note 1, at 61.

¹⁴ PHAIR, *supra* note 1, at 83.

¹⁵ PHAIR, *supra* note 1, at 83.

¹⁶ PHAIR, *supra* note 1, at 86; *see also* The Associated Press. *The U.S. Plan on Net Computers Draws Mixed response*, www.usatoday.com 2 July 2005.

¹⁷ PHAIR, *supra* note 1, at 92.

¹⁸ PHAIR, *supra* note 1, at 92.

Finally, the author introduces a proposal for enforcement of cyber crimes, in light of the fact that it is a global issue that affects all international jurisdictions. First, he proposes “to control the incoming backbone, the part of the internet’s infrastructure that is within an economy’s national territory; secondly, to establish a law enforcement regime that can police the Internet; and thirdly, attempt to establish regimes of rights and duties between citizens in the safe and proper use of Internet technologies.”¹⁹ The author goes into depth as to how countries should achieve this proposal, and notes that law enforcement agencies currently play a small role in the prosecution of cyber crimes because of the low level of reported incidents.²⁰ As a Federal Agent, the author brings a very realistic approach to the prosecution of cyber crimes and what steps governments should take in order to prosecute these crimes.

Cybercrime: The Reality of the Threat is an excellent source for introductory material to the area of cyber crime. The author provides a general overview of nearly all of the important areas of cyber crime, how they are defined, how they are committed, with what tools and by whom, and provides concrete examples and case law. Throughout the book, he draws attention to the vulnerabilities of using the Internet and the protections that one must use to safeguard himself. The message is established; that individuals, governments and corporations must take “all reasonable precautions” to protect themselves from becoming the victims of cyber crimes.²¹

¹⁹ PHAIR, *supra* note 1, at 153; see also NATIONS S. HEDLEY, *MARKETS AND OTHER IMAGINARY PLACES: WHO MAKES THE LAW IN CYBERSPACE?* INFORMATION AND COMMUNICATION LAW, VOL 12, NO, 3, OCTOBER 2003.

²⁰ PHAIR, *supra* note 1, at 156.

²¹ PHAIR, *supra* note 1.