

Computer Network Security and Cyber Ethics

Written By Joseph Migga Kizza

Reviewed by Kathleen E. Lang

Computer Network Security and Cyber Ethics by Joseph Migga Kizza addresses the sobering, on-going Internet-related security concerns of network administrators, such as the various forms of cyber attacks that necessarily confront an Internet-dependent, global society. The author stresses that together with the almost magical freedom of a cyberspace infrastructure, namely the Internet, come costs associated with cyber crimes, cyber crime prevention and network recovery. Cyber attacks are only increasing and are unchecked by current cyber security measures. Kizza predicts an avalanche of cyber-vandalism as the world becomes increasingly dependent on computer networks.

Cyber crimes and cyber-vandalism can potentially affect anyone using the Internet, and Kizza seeks to educate a broad spectrum of people about the magnitude of such crimes and the weaknesses inherent in a cyberspace infrastructure. Kizza does this by giving a general background to the underlying motives of cyber attacks, detailing how the attacks are committed, and what efforts are underway to prevent future attacks. The author hopes that a cyberspace security policy will educate the public about cyberspace vulnerability, and ensure that the public is equipped to deal and possibly prevent cyber attacks. According to Kizza, a legal and regulatory framework needs to be created to handle the consequences of living in a cyber-society. Kizza's anticipated audience includes computer network security personnel and policy makers; students in computer science, information science, technology studies, library sciences, engineering, and information technology; or anyone that hopes to become computer literate. Kizza intends

that the book will be used as a teaching and reference tool and includes general exercise questions for classroom use at the end of the book.

There is a definite need for a book like *Computer Network Security and Cyber Ethics*. Cyberspace infrastructure and communication protocols by their nature are weak, and average users have no idea of the “gaping loopholes” in security when they access the Internet. Society is becoming increasingly dependent on cyberspace and therefore vulnerable to these loopholes. Kizza regards society’s attitude as complacent towards hackers, regarding them simply as ‘whiz kids’ instead of as criminals. The only remedies implemented for cyber attacks so far have been case-by-case patches, and not widespread research for better solutions to the underlying problems. Reporting of cyber attacks is voluntary and random. The nation does not yet understand the seriousness of such attacks or the associated costs. Kizza does an excellent job sounding the alarm, and suggesting policies to correct the situation.

The author begins his book with the chapter *Cyberspace Infrastructure*, which describes communication protocols and networks, giving the reader a basic understanding of networks in general and the Internet specifically. This enables the reader to dissect the *Anatomy of the Problem* in the second chapter. In this chapter, Kizza addresses types of cyber attacks, and the costs and social consequences of cyber crimes. He also discusses how to prevent, detect and survive cyber crimes, while addressing the nature of cyber-ethics in today’s world and tomorrow’s.

Kizza cites a 1997 estimate that the U.S. economy loses more than \$100 billion each year through industrial espionage, which has grown 500 percent since 1992. To date there are inadequate protections from attacks, and at least two-thirds of computer

firms do not report hacker attacks for fear of economic and physiological impacts, such as lack of consumer confidence. Most countries, including the United States, do not have mandatory reporting requirements. The Department of Defense reports that a victim detects only one successful attack in twenty, and that almost ninety percent of computer attacks are from within an organization. Businesses typically respond to these attacks with patches, filters, and other solutions. Kizza does a good job of pointing out the social and ethical consequences of cyber attacks as well, such as the loss of privacy from documented 'e-attacks attacks' on CNN, eBay, E*Trade, and Amazon, and other global email attacks.

There is commonly a lag between developing technology and legal processes to protect users of new technologies or to prosecute violations. This problem is made worse because of the Internet's international reach. Kizza notes that there are approximately 30,000 hacker-oriented websites that disclose hacker know-how and tips on how to create computer viruses or "bugs." One virus, the Manila-generated "Love Bug," virtually circumnavigated the globe in twelve hours, illustrating that a teenager with Internet access in an underdeveloped nation can wreak as much cyberspace havoc as a privileged teenager in a developed nation. This creates a difficult situation for law enforcement. Indeed, the Philippines have no computer crime law, making it extremely difficult to arrest the "Love Bug" hacker.

Kizza illustrates that the rise in e-attacks has prompted collaboration between public and private industries to warn the public of cyber-intrusions and to attempt to remove vulnerabilities. The last chapter generally describes the cyberspace-related "hot issues" like cyberspace access and growth, Internet governance, security, privacy,

copyright, free speech, and intellectual property rights. Kizza notes that a “digital divide,” or unequal access to information, results from differences in geography, income, race, age, and education. Regardless, he notes that privacy policies must be developed to protect all customers’ privacy, regardless of income, race and geography, and to foster international business on the Internet.

Kizza attempts to educate the public about cyberspace security issues in this easy to understand computer reference book without sounding like an alarmist. Though brevity is appreciated in any reference book, this reader would have appreciated more details on cyber attacks, including how much each attack costs, and how such costs are allocated. Instead, Kizza’s last chapter, *Cyberspace and Cyber Ethics Today and Beyond*, glosses over hard-hitting facts and vouches for public education even though he admits that this is a long-term initiative. Kizza cites the need to establish a legal and regulatory framework because the Internet will increasingly become a venue for criminals as it has already become one for hate groups, pedophiles, gamblers, money launderers and so on. Kizza warns that the public must be educated to guard against personal identity theft and misuse of information because computer networks in general readily allow for such violations of privacy. *Computer Network Security and Cyber Ethics* is a good reference book for a novice seeking general information on computer networks, intellectual property, and issues surrounding society’s uninhibited Internet use