College of Business book Review by Dan Clapper

Title: "Creeping Failure: How We Broke the Internet and What We Can Do To Fix It"

Authors: Jeffrey Hunker

Publisher: McClelland and Steward

Length: 270 pages

Price: $25.95 (hardback)

Reading time: 10 hours

Reading rating: 2 (1 = very difficult; 10 = very easy)

Overall rating: 3 (1 = average; 4 = outstanding)

In “Creeping Failure: How We Broke the Internet and What We Can Do To Fix It” Jeffrey Hunker shows how inherent design problems, lack of incentives, and the current legal and regulatory environments have led to the failure of the Internet to provide the security for the economic and social transactions on which businesses and consumers increasingly rely.

In examining the nature of this failure, the author suggests that rather than being a catastrophic failure due to a glaring mistake or grand miscalculation, the Internet is instead succumbing to a creeping failure – a gradual failure due to problems that we either can't cure or have neglected to cure.

One important driver for this is the changing nature of computer hacking. The author contends that between 2001 and 2004 computer hacking morphed from being a rebellious, individual effort to a valuable revenue source for criminal enterprises – a shift from geeks to gangsters. In this timeframe hacking skills were increasingly co-opted by a new type of organized crime intent on using the Internet as a new means for expanding criminal activities.

One indication of this change is in the exploding number of viruses. The author reports that in 2002 and 2003 Symantec created about twenty thousand new ‘malicious code signatures’ each year. This means that about twenty thousand different viruses and other malware were detected and digitally fingerprinted for inclusion in the firm’s anti-virus software. In 2008, the same company created over 1.6 million new malicious code signatures.

This situation is enabled by the fact that the Internet was never really meant for secure transactions. The early designers of the Internet never envisioned anything like the global, commercial and social network phenomena the Internet has become. The underlying architecture was not designed for this and consequently, the author contends, our current Internet is just not able to deliver on the need for security.

Weaknesses in the fundamental design of the Internet along with the changing nature of criminals use of the Internet has profoundly changed the nature of cyber crime. And unfortunately, the author says, the world's cyber-security policies -- its laws and regulations -- have not kept up. Technology alone cannot solve this problem; instead the author suggests that user expectation must be changed and new policies must be developed to stop this creeping failure.

The book suggests that a new ‘social contract’ is needed to change user expectations. Currently the social contract for the Internet is "the Internet is free and I'll do whatever I want to do on it”. The author suggests that in public health and safety, societies recognize the collective need to sacrifice some aspects of personal flexibility and privacy for the common good. These solutions have become such an accepted part of our lives that we don’t even recognize them as solutions anymore (it’s hard to imagine early subscription fire fighting companies that would only respond to members’ fires), but these solutions can provide new ways to think about how to balance individual freedoms with the collective good.

The author suggest four broad approaches to improving the security of the existing Internet: A new framework for Internet governance, tort liability for software vendors and network service providers, a robust insurance market, and better security data collection that would support tracking and prosecuting cyber crime.

None of this is quick or easy -- it represents a significant change in our expectations about how we should use, govern and police the Internet. While no silver-bullets are provided, this book provides an excellent description of the daunting problem of Internet security and some of the long-term changes that may be required to fix it.

Dan Clapper is an associate professor of computer information systems in the College of Business at Western Carolina University. He teaches application development for both the desktop and Web environments. For previously reviewed books, visit our web site at www.wcu.edu/cob/.