BOOK REVIEW

Chasing Shadows: The Human Face Behind the Cyber Threat

Tangled Web: Tales of Digital Crime From the Shadows of Cyberspace, Richard Power, Que, 2000, 450 pages.

Jim Christy*

Richard Power's *Tangled Web: Tales of Digital Crime From the Shadows of Cyberspace* presents one of the most comprehensive computer crime accounts available. The book unveils and explores in meticulous detail the present nature and scope of computer crime, and—more importantly—the tremendous potential that common criminals, terrorists, and nation-states now have at their fingertips.

Tangled Web offers a detailed account of the *Citibank* caper—a landmark case widely regarded as the most important computer crime ever committed—in which hackers from St. Petersburg, Russia, electronically hijacked $10,000,000.[1] The case was the first and only time a bank has admitted to an electronic hacking and resulting theft of money. Power's definitive investigative summary follows the crime in detail, from its accidental discovery by a South American Citibank customer to the identification and arrest of the perpetrators. Many questions have never

* Mr. Christy has been a computer crime investigator for the past fourteen years, and is currently with the Department of Defense. Mr. Christy served as the Defense Department representative to the President's Infrastructure Protection Task Force ("IPTF"), prior to which he served as a Congressional Fellow on Senator Sam Nunn's staff on the Senate Permanent Subcommittee on Investigations.

1. Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 472 (Summer 1997).

been answered, however, and several unsolved mysteries still revolve around this case.

Power is the first to appropriately credit retired Senator Sam Nunn as the person responsible for drawing the attention of both the government and the private sector to this critical security issue. Senator Nunn chaired the 1996 "Security in Cyberspace" hearings before the Senate Permanent Subcommittee on Investigations—the impetus for the tremendous amount of positive change in the legislation of digital crime in the last four years.

The Permanent Subcommittee on Investigations was the first congressional committee to hold hearings that outlined the threat to national security from cyberspace. Computers and networks control critical elements of society's infrastructure, like telecommunications, electrical power, gas and oil production and distribution, water, banking and finance, and emergency services—illustrating the tremendous importance of maintaining a secure cyberspace. These hearings were the first to describe the vulnerability of the most powerful nation in the world, not only to nation-states and terrorists, but even to "ankle biters."[2] Our dependence on the very technology that created the recent boom in our economy now constitutes our nation's Achilles heel.

President Clinton selected the "Security in Cyberspace" hearings as the forum to announce this nation's first policy initiative to protect our critical infrastructure, emphasizing the need for protection from cyber threats.[3] The President asked Deputy Attorney General Jamie Gorelick and Deputy Secretary of Defense John White to announce the previous day's signing of Executive Order 13010, creating the President's Commission on Critical Infrastructure Protection ("PCCIP" or "Commission"), and the President's Infrastructure Protection Task Force.[4]

The PCCIP, comprised of ten government commissioners and ten private-sector commissioners, studied the vulnerability of the nation from both physical and cyber attack and offered recommendations to the President.[5] The resulting recommendations described the PCCIP's national policy proposal and set forth a strategy to implement them. Following his

2. NEWTON'S TELECOM DICTIONARY, 60 (16th ed. 2000) (defining "ankle biter" as "a person who aspires to be a hacker/cracker but has very limited knowledge or skills related to computer systems. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet").

3. Exec. Order No. 13,010, Fed. Reg. 37,347 (July 15, 1996).

4. *Id.*

5. *Id.*

retirement, Senator Nunn was named a co-Chairman of the PCCIP's Advisory Committee along with Gorelick, the Commission's private-sector advisor.

On the basis of these recommendations, the President issued Presidential Decision Directive 63 ("PDD 63") in May 1998, outlining the National Plan for Critical Infrastructure Protection. Thus, all of the current national policy on Information Assurance and Infrastructure Protection began with the precedent-setting Senate hearings chaired by Senator Nunn.

Richard Power played no small part in those precedent-setting Senate hearings, offering testimony about the first-ever "Computer Crime and Security Survey."[6] Power was a critical witness who helped to urge Congress and the Clinton administration to take these very important steps to protect our national defense, national security, and economic security. Power's computer crime survey was the first of its kind, particularly featuring data from the private sector on cyber crime.[7] Encouraging the private sector to share information concerning its vulnerability to cyber crime was critically important. The computer crime survey played a vital role in collecting and assembling the data that convinced the government that computer crime posed a very real threat to national and economic security. Power was selected to provide Senate testimony on his computer crime survey findings because of his personal reputation and the validity of his data.

In *Tangled Web*, Power correctly focuses on the threat of computer crime, as well as its solution. The threat is not a technical one and the solution is a simple one. The threat is not the computer, but fingers on the keyboard. The solution is blatantly obvious and simple—people. information technology managers must understand and counter the very real human threat to cyber security with appropriate resources, policies, and punishments.

In every one of Power's case studies, the text makes very clear that the perpetrator is a person, a human. Having participated in many conferences and workshops through the years that addressed the threat, I have heard and debated with some very intelligent people about where the threat really comes from. Many in the information technology field believe

6. *Security in Cyberspace: Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs*, 104th Cong. 75-84 (1996) (testimony of Richard G. Power).

7. *Id.*

that the threat is a technical threat. These tend to be the more technically oriented people, and they try to counter the threat with a technical fix.

Power rightly identifies the threat as the human that creates and executes the technology he has created. More importantly, the most effective defenses against this threat are also human—the educated user who is careful to avoid unintentionally causing problems, or the vigilant user who detects anomalies and reports them.

Government and business will never have the resources to do the necessary research and development of technical countermeasures to effectively defend their systems. Even if the externalities remained stagnant, the costs would be overwhelming and, therefore, prohibitive. A network lives, breathes, and literally changes daily with the introduction of new software, new hardware, and changes to network configuration. Defending a network is like defending a moving target.

The intruder need only find one network vulnerability to exploit. The defender, by contrast, must find and fix all of the vulnerabilities. This human defender must develop, implement, and enforce good policies, then develop the technologies that will be deployed to enhance the security posture. When all the securities fail and a system falls victim to an intruder, a competent cyber cop must be able to successfully investigate and collect the necessary evidence that will identify the perpetrator and support the prosecutor. From start to finish, the entire process depends on humans.

Technology will never be able to prevent or detect the privileged user, the systems administrator, or the network administrator that goes bad. The privileged user—the insider—poses the greatest threat to our systems, and technology will never be able to keep this threat in check. Only policies and enforcement of those policies by dedicated humans can address this insider problem.

The intricacies and nuances of the case studies that *Tangled Web* features were impressive. Power detailed several comprehensive, lesser-known cases. Particularly striking, the number of cyber cops today has skyrocketed compared to when I started as an investigator. In the old days—five to ten years ago—we all knew one another. There were probably less than fifty cyber cops worldwide. Today, federal, state, and local law enforcement agencies are starting to recognize the need for hybrid criminal investigators able to successfully recognize and investigate the crimes of today and tomorrow.

Tangled Web is a must-read for all cyber cops, prosecutors, and information technology heads and policy-makers. It's not just the ankle

biters roaming cyberspace anymore.