Cybercrime: Criminal Threats from Cyberspace

By Susan W. Brenner
Price $45.00, pp. 281

Reviewed and Interviewed by Anna Cometa
Journal of High Technology Law
Suffolk University Law School

“Some day, every crime is going to be a cybercrime.”¹

Professor Susan W. Brenner’s² fascinating new non-fiction, Cybercrime: Criminal Threats from Cyberspace,³ provides the reader with a real-world depiction of the evolution of cybercrime and the current domestic and international risks posed by cybercriminals. Brenner tells this story through the use of real world cases, ranging from a handicapped teenager who used his knowledge of computers to threaten a town 1,000 miles from his home, to hackers who gained access to Air Force bases and government security databases in the United States, Mexico, South Africa, and Europe.⁴ With rapidly growing computer technology, security systems became even more sophisticated to combat the cybercriminals.

Anyone who reads Cybercrime will be introduced to a new type of criminal or one that has merely been overlooked for decades. This is a criminal who can terrorize people, steal their personal information, and shut down their government security systems from the comforts of his or her home. See below for an interview of Professor Brenner, her personal thoughts about

¹ SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE, 37 (quoting the thoughts of police officer colleagues).
² Susan W. Brenner is the NCR distinguished professor of law at the University of Dayton School of Law in Dayton, Ohio. She specializes in grand jury practice and cyberconflict which includes cybercrime, cyberwarfare, and cyberterrorism.
³ See BRENNER, supra note 1, at 37.
⁴ See BRENNER, supra note 1, at 3, 139-41.
cybercrime, and a behind-the-scenes glimpse of what went into writing \textit{Cybercrime: Criminal Threats from Cyberspace}.

\textbf{JHTL: First, I’d like to thank you on behalf of Suffolk University Law School and the Journal of High Technology Law for taking the time to let us interview you. Could you tell us a little bit more about your background?}

SB: Before I became a professor at the University of Dayton School of Law, I was with a Chicago law firm Silets & Martin, Ltd. that specialized in federal white-collar criminal defense. The experience left me with an interest in “complex crimes”—crimes like RICO that encompass new and/or distinctively complex criminal activity. Federal white-collar defense often involves a lot of motion practice in which defense attorneys target the structure of the offenses the prosecution has included in an indictment in an attempt to get as many charges as possible dismissed. So, I came to law teaching with an interest in what you might call the outer boundaries of criminal liability.

\textbf{JHTL: What inspired you to write about cybercrime and the risks associated with attacks by cybercriminals?}

SB: I taught my first class, a seminar in cybercrime in 1997, because it was already apparent that cybercrime was an important emerging phenomenon. The next year I taught an online (completely online) seminar in Cybercrime Law, which included many outside experts in the area (many from the U.S. but some were from Europe). I taught that class for about seven years, published some articles in the field, and began to be invited to speak at conferences and write
articles on cybercrime issues. So, I’ve been writing in the area for well over a decade. The cybercrime book is really the culmination of a lot of work I’ve been doing for a long time.

**JHTL: Have you ever been a victim of cybercrime? (My computer got a debilitating virus last week…)**

SB: No . . . knock on wood (or on a hard drive) . . . I haven’t been a victim, yet anyway. Don’t feel bad, though. Many, many people have been victims of cybercrime.

**JHTL: Part of how you illustrate the reality of cyber threats in *Cybercrime* is through real-life anecdotes. What do you want your audiences to take away from reading these stories?**

SB: I use anecdotes – all of which involve real-life cases – because they help readers who know nothing about cybercrime understand what it is and how it differs from traditional crime. So, if I talk about the case in which foreign cybercriminals siphoned nearly half a million dollars out of a bank account belonging to a U.S. county, that helps to illustrate the differences between the twenty-first century cyber-bank robber and the twentieth century, Bonnie & Clyde version of the crime.

**JTHL: As technology-related crime increased significantly with the evolution of the Internet and computer technology in the 90s, the government and public fear seemed to play a major role in the effort to prosecute and legislate against cybercriminals. In 2011, however, do you think the public has become somewhat desensitized to cybercrime?**

SB: I think the public is, for the most part, blissfully unaware of cybercrime. Security professionals are VERY aware of it, as are the law enforcement officers (and prosecutors) who
work in this area. But, if you notice, you see few very news stories – online or on TV – that deal with the complex cybercrimes . . . the cases in which foreign criminals extract hundreds of thousands or millions of dollars from U.S. bank accounts or extract personal identifying information (credit card numbers, Social Security numbers, etc.) of U.S. citizens from U.S. databases and either use it themselves or sell it to others who use it to profit. One of the reasons why these stories seldom, if ever, make the mainstream media is that the victims – the banks and businesses that are targeted – have absolutely no incentive to report their being victimized. After all, how many of us want to do business with a bank that’s had funds extracted by cybercriminals? We want to believe the institutions we deal with are safe.

**JHTL:** In your opinion, what legal recourse should be in place to deter cybercriminals? Do you think it is impossible to deter someone who has the ability to commit crimes anonymously and in the comfort of their own home?

**SB:** Pretty much . . . if you’re in another country and you can commit cybercrimes with very little chance of being caught, extradited, and punished for your crimes . . . while making very good money, why would you not do so? It’s got to be a particularly attractive alternative for talented computer experts who are in countries where it may be difficult for them to find a legitimate computer job and if they do, the job may pay very little. I also think many foreign cybercriminals are oblivious to the “harm” they inflict on us, since people in the U.S. tend to be regarded as fabulously wealthy (like the people who generally populate our movies and TV shows). If we’re wealthy, it follows that we won’t really feel a few losses, which might salve a cyber thief’s conscience. As for legal recourse, the logical option would be a global cybercrime
agency that pursues cybercriminals wherever they’re located . . . but we all know that isn’t going to happen (and I’m not sure that I, for one, would be comfortable with such an agency).

**JHTL: Towards the end of the book, you write about the tradeoff between privacy and national security. Do you envision policymakers taking either direction going forward?**

SB: Well, online privacy is a conundrum . . . if I post information on my Facebook page or on my blog, how can I say it’s private? And if I send unencrypted emails – which are the functional equivalent of postcards, since ISP employees can read them – how can I claim they’re private when postcards aren’t? I think we (notably the Supreme Court) need to re-conceptualize privacy in an era of pervasive digital technology . . . which is, of course, easier said than done. I also work in the area of cyberwarfare, which is equally depressing. My fear, which is shared by many knowledgeable people, is that we’ll have a major cyberattack – a cyberterrorist event analogous to 911 or an attack from a hostile nation-state – and then we’ll overreact in various ways, one of which might be to cut back on privacy.

**JHTL: What can civilians do to secure their information in light of the growing sophistication of hackers, identity thieves and other cybercriminals worldwide?**

SB: Well, the usual . . . use virus protection, don’t put anything online you don’t want others to know about, password-protect everything you can . . . and most importantly, be cautious. One of my theories is that people tend to be victimized more online than in the physical world because they don’t take the online world as seriously as the physical world. If a Nigerian prince approached John Doe in the real world and offered him $15 million for helping the prince extract $100 million from a bank account in some African state – which involved conduct that was only
slightly illegal – I’m sure John Doe wouldn’t buy it . . . but a lot of John Does buy that scam when it’s online.

**JHTL: What advice do you have for legal professionals who are interested in working on these issues?**

SB: I think it’s a growth area. There aren’t a lot of jobs right now for cybercrime prosecutors, I’m afraid. There are cybercrime prosecutors in the federal system, in many state Attorneys General’s offices and in some county prosecutors’ offices, but those opportunities are limited for the moment. Cybersecurity is a major concern in business, so there might be jobs there; since I focus on the criminal aspect of all this, I’m not particularly knowledgeable about that sector.

There are defense attorneys who handle cybercrime cases, but I don’t know of any who specialize in those cases, at least not yet. I should mention one other aspect of cybercrime: the general federal cybercrime statute creates a civil cause of action for anyone injured by conduct that violates the statute, which generates quite a bit of civil litigation. These cases are usually filed by businesses that have been victimized by disgruntled employees, rival companies, and the like. Since the cases involve seeking damages for the commission of federal cybercrimes, the lawyers who litigate them have to understand cybercrime law, even though they may never handle any criminal cases.

And, as I said, it’s a growth area. I think we’ll see more and more emphasis on cybercrime. About a decade ago, when I would talk to law enforcement officers who worked in this area, they’d say, “someday every crime will be a cybercrime,” i.e., every crime will involve the use of computers and the Internet. We’re getting pretty close to that, even traditional crimes like murder and drug dealing involve the use of computers.
JHTL: Thank you so much for talking with us. I really enjoyed reading your work. It is a fascinating and important read for anyone whose life is affected by technology (whose isn’t, nowadays?). Cybercrime poses serious domestic and international risks and I hope that we see some effective developments in how to regulate this type of activity in the future.