Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

Cyberwhatsit

I did a Google search on the word *cyber* and was told there are 467 million references to that term. This seems to me an awfully exact number, but I guess we can agree there are a lot of references. But references to what exactly? Cyber*crime*? Cyber*attacks*? Cyber*threats*? Cyber*security*? For fun, I looked at the 20th page of the Google search and found cyberrisk, cybercareer and cybercafe. Languages (well, English anyway) have an enormous capacity for newspeak through the combination of an adjective and a noun. This little linguistic interlude would be an interesting aside, except that I think it points to a genuine obstacle to progress in countering the problems connoted as cyber. We need targeted countermeasures to the targeted threats posed by Internet-enabled terrorists, state-sponsored spies and saboteurs, misguided political activists, and criminals. A lack of verbal clarity is not going to help.

There is, I believe, a correlation between fuzzy speech and fuzzy thinking. If we are not clear about what we consider the problem to be, we are more likely to be off-target in developing the necessary solutions. Objectives matter. No matter how great the risk of directed misuse of information resources, budgets for mitigating those risk factors are limited and those responsible for safeguarding those resources can ill afford applying the allocated money inappropriately.

CYBERTHEFT

Donn Parker, perhaps the earliest chronicler of crimes committed by computers, suggested many years ago that even automated murder was possible.[1] And indeed, if a life-support system is computerized, would not disabling its system constitute the ultimate felony? However, in the current usage, the term cybercrime is generally applied to stealing information. And, even that takes several forms. The one that seems to make it into the headlines most often is the theft of personally identifiable information (PII), especially information that can be readily monetized, i.e., credit card numbers and authenticators. Target and Home Depot have been recent and well-publicized victims of such crimes, which are, in actuality, privacy violations. As such, I propose that the tools of privacy protection, such as encryption, compartmentalization and disposal, are best applied to stop this sort of theft.

There is another type of cybercrime that I consider even more insidious: theft of proprietary information. Gen. Keith Alexander, director of the US National Security Agency (NSA) and commander of the US Cyber Command, has said that the loss of industrial information and intellectual property through cyberespionage constitutes the "greatest transfer of wealth in history."[2] He ought to know. Once again, encryption is probably the tool of choice, but since the information needs to be decrypted to be used, encryption is an incomplete solution. If the information is as valuable as Gen. Alexander implies, perhaps it should be kept on separate, classified systems as is done in the military.

Criminals do have another way of making cybercrime pay, by stealing information assets that have intrinsic value. Sony has recently been victimized in this way.[3] The only sure way to protect valuable property is to lock it in a vault. In computer terms, this means not storing information resources that are valuable in themselves on Internet-accessible devices.

CYBERATTACKS

To my way of thinking and speaking, an attack—cyber or otherwise—implies intent to harm a person or organization. Stealing information is harmful, to be sure, but it does not undermine an organization's essential business functions. I reserve the word *cyberattack* for cases in which an organization is prevented from carrying out its intended mission. Cyberattacks threaten the integrity or the very existence of information and have the potential to bring a business to a halt. When Saudi Aramco and RasGas were attacked in 2012, up to 30,000 computers were wiped clean, replacing their contents with the image of

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

a burning American flag. These attacks were linked to Iran.[4] Such destructive attacks can only be combatted, to my way of thinking, by adopting zero-trust architectures based on next-generation firewalls.[5]

A variant on destructive attacks is one in which the integrity of a system is violated. Perhaps the most notorious of these was Stuxnet, malware originated by Israel and the US, according to many sources, including Edward Snowden, formerly of the NSA.[6] He ought to know. This attack was designed to "physically damage the facility's infrastructure by throwing off automated systems and cover its tracks so that even if engineers were monitoring those systems, everything would appear normal."[7] I have previously advocated frequent validation of the integrity of software,[8] which might have arrested the damage of Stuxnet. One might say that all cyberattacks on software or information integrity are failures of change management, so strengthening these controls is also a tool against cyberattacks.

> We can only win if we fight the right fights with the right tools against the right enemies.

CYBERTHREATS AND CYBERSECURITY

We live in threatening times that these malefactors of great stealth have bestowed upon us. It is what Thomas Friedman of *The New York Times* calls "the struggle between 'makers' and 'breakers' on the Internet."[9] I have confidence that we who make and protect information systems will win out in the end. But let us not overlook the depth of resources, talent and time that the breakers have at their disposal.

We can only win if we fight the right fights with the right tools against the right enemies. **Figure 1** summarizes the cybertaxonomy (aha, another cyberneologism…and another!) discussed above.

It demonstrates that the cyberthreats are not all the same; they come from different sources, each with different impacts and safeguards. We set back the cause of the makers by treating cybersecurity as a monolith. One size fits nobody. The breakers are not all alike and the response by the makers must be nuanced as well. If we are clear in our minds as to whom and what we are fighting, we are a great deal more likely to win.

Figure 1—Different Types of Cyberthreats

Types of Assault	Intended Effects	Probable Sources	Recent Victims	Selected Countermeasures
Stealing PII	Credit card fraud; blackmail	Criminals	Target, Home Depot	Encryption, compartmentalization, disposal
Theft of intellectual property	Industrial espionage	Governments, hacktivists	Sony	Encryption, classified systems
Theft of valuable information resources	Piracy	Criminals	Sony	Segregation, air gap
Destructive attack	Destruction of information	Governments, terrorists	Saudi Aramco, RasGas	Zero-trust architecture, next-generation firewalls
Integrity attack	Manipulation of systems or data	Governments, terrorists	Iranian nuclear program	Software validation, change management

ENDNOTES

[1] Kearns, Helen; "The Dawn of Computer Crime: Theft Today…Is Murder Next?," *Montréal Gazette*, 17 May 1978, *http://news.google.com/newspapers?nid=1946&dat=19780517&id=_DgyAAAAIBAJ&sjid=b6QFAAAAIBAJ&pg=4051,330681*. This article quotes Donn Parker, the bald eagle of information security and someone I consider a friend and a mentor. He was talking about cybercrime before most of us could spell cyber.

[2] Rogin, Josh; "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy*, 9 July 2012, *http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/*

[3] Barnes, Brooks; Nicole Perlroth; "Sony Films Are Pirated, and Hackers Leak Studio Salaries," *The New York Times*, 2 December 2014, *www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html?module=Search&mabReward=relbias%3Ar*

[4] Perlroth, Nicole; "Report Says Cyberattacks Originated Inside Iran," *The New York Times*, 2 December 2014, *www.nytimes.com/2014/12/03/world/middleeast/report-says-cyberattacks-originated-inside-iran.html?module=Search&mabReward=relbias%3Ar*

[5] Beck, Eric J.; "How Zero-trust Network Security Can Enable Recovery from Cyberattacks," *ISACA Journal*, vol. 6, 2014, p. 14-18, *www.isaca.org/journal*. Full disclosure: Eric Beck is my business partner at Risk Masters.

[6] Ferran, Lee; "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet," *ABC News*, 9 July 2013, *http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/*

[7] *Ibid*.

[8] Ross, Steven J.; "CyberCERT," *ISACA Journal*, vol. 5, 2014, *www.isaca.org*

[9] Friedman, Thomas; "Makers and Breakers," *The New York Times*, 8 November 2014, *www.nytimes.com/2014/11/09/opinion/sunday/thomas-l-friedman-makers-and-breakers.html?module=Search&mabReward=relbias*