The Cyber Underground Economy: Unconventional Thinking for a Fundamentally Different Problem

By Gene Loughran and Frank Strickland

Thinking Differently about Cyber

Government officials have warned of the potential for a cyber Pearl Harbor that paralyzes one or more critical components of the country's public and private infrastructures. In April 2011, a cyber attack crashed 30 servers at a South Korean bank, destroying data and eliminating financial services for several days. If North Korea was responsible for the attack, as South Korean officials have asserted, it demonstrates how one of the world's most impoverished nation-states can use cyber to successfully attack one of the world's most prosperous. This would seem to increase the possibility of a digital Pearl Harbor as both rational and rogue state actors acquire cyber warfare capabilities. This conventional thinking could, however, obscure a much greater danger in the near term, one that threatens our economic recovery while feeding on an underground economy.

Noah Shachtman, contributing editor at *Wired* magazine and non-resident fellow at the Brookings Institution, argues in a recently published study that the cyber danger better resembles neighborhoods controlled by criminal elements, making it difficult for honest people to live and work there. Cyber crime is fueled in no small part by an underground economy wherein criminals buy and sell the information, tools, and techniques used in cyber crimes[1].

Government leaders should consider whether the top cyber threat is a digital Pearl Harbor—whatever that means in practical terms—or the high-tech underworld, especially at a time when the American and global economies can ill afford substantial drain from illegal activities. While the responsibilities for dealing with crime and underground economies have traditionally fallen to law enforcement officials, a wider range of government leaders should understand the underground cyber economy. The weapons and tactics created there could be used by amateurs and sophisticated actors to attack public information, services, and infrastructure. Moreover, while law enforcement takes the lead in confronting the underground cyber economy, solutions will likely involve a wider range of public and private-sector groups working together in structures and modalities, most of which do not exist today.

The Nature of the Cyber Underground Economy

The cyber underground economy—a collection of virtual marketplaces where cyber criminals buy, sell, and trade goods and services—continues to thrive even in the challenging global economic climate. At the heart of the cyber underground economy are computer hackers. Groups of young computer enthusiasts—motivated by the challenge of accessing restricted networks—formed the earliest cyber criminal gangs in the 1980s.[2]

Almost two decades later, technology and network speeds have advanced substantially, enabling an explosive growth in electronic commerce or e-commerce—with billions of dollars traversing the World Wide Web (WWW) each day. Cyber crime, too, has matured —increasing in expertise, sophistication, and organization. No longer a teenage hacker trying to get free phone calls, the modern day cyber criminal is organized and calculating.

Goods sold on the cyber underground primarily consist of payment card information (PCI) such as credit card numbers, PINs, and bank account credentials, personally identifiable information (PII) such as e-mail accounts, addresses, and social security numbers, and enabling items such as crimeware. However, the criminal is interested in any information that can be exploited for profit.[3] Services include providing mules that can turn stolen accounts into currency, phishing campaign management, web hosting, development services, and botnet leasing.[4]

The cost of goods and services in the underground economy ranges from two U.S. dollars for a U.S. credit card (CC) dump with card verification value to several hundred U.S. dollars per month for botnet rentals to $3,000 for crimeware like the Zeus Sploit-Pack, a popular botnet exploitation package.[5] With these tools and services, anyone from another

Gene Loughran, Senior Managing Consultant, leads advanced mission analytics work for cyber and several other national security missions. Gene has led several breakthroughs in assessing the value of information and IT, most recently for the U.S. Central Command's communications architecture in the war zones. Gene is a Certified Information Systems Security Professional (CISSP) and holds the CIO University's certification in federal executive information competencies.

cybercrime syndicate or gang, a terrorist group, or a nation-state can conduct criminal activities such as fraud, laundering money, or stealing identities and secrets.

Cyber crime takes many forms, and most, but not all, have some interaction with the cyber underground economy. This article focuses on major cyber crime issues that directly affect the global economy and include computer intrusions; fraud as it relates to financial services; theft of identities, credit cards, credentials, or trade secrets; and operation of the economy in which these goods and services are bought and sold.

The actual size of the cyber underground is difficult to estimate. One approach is to look at costs associated with reported losses as a baseline measure. Over the last 10 years, complaints reported to the Internet Crime Complaint Center (IC3) increased nearly twentyfold, with damages estimated at around $559.7 million.[6] However, according to a presentation given by Peter Guerra at the 2009 BlackHat Conference in Las Vegas, Nevada, estimated losses due to cyber crime range widely and may be much higher.

What is clear is that the growth of cyber crime over the last decade, in terms of dollars lost, has been enormous. Considering the vast numbers of compromised accounts potentially available for sale in the underground economy (over 130 million credit card, debit card, and bank account credentials stolen or lost in 2009 in the U.S. and Canada), current estimates placing the global cyber underground economy in the tens of billions of U.S. dollars are entirely plausible.[7]

Participants in the Cyber Underground Economy

Over the course of 30 years, cyber crime has evolved from teenage pranks to a well-oiled, organized criminal economy. Organized crime, as used here, means cyber crime groups with some sort of organizational structure and does not imply that traditional organized crime groups are involved in a meaningful way in the cyber underground economy. In fact, there is only scant evidence of this type of involvement.[8] ShadowCrew and DarkMarket were two major carding forums that illustrate organized cyber crime.

ShadowCrew, whose organization was modeled on the Italian Mafia, boasted more than 4,000 registered members; DarkMarket had more than 2,000. The U.S. government estimated that ShadowCrew was responsible for an estimated $4 million in losses[9] due to its criminal activities. Both ShadowCrew and DarkMarket harbored an economy of underground cyber criminals who bought, sold, and traded goods and services used in identity theft, spam, fraud, and other illicit activity.

Albert Gonzalez, a rising star in the organized crime gang known as ShadowCrew, came onto the scene in 2003 when he was caught using blank debit cards with stolen card numbers (presumably from the ShadowCrew carder forum) to withdraw hundreds of dollars in cash. After a stint as a U.S. Secret Service informant, Gonzalez returned to a life of crime, enlisting the expertise of programmers and criminals he knew to build a small group that would ultimately

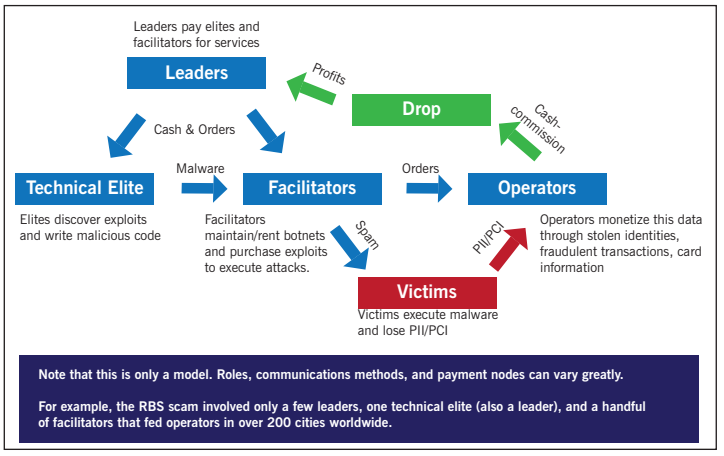

Figure 1. Cyber Underground Economy, Roles and Relationship Model (IBM)

Frank B. Strickland is a Senior Fellow with the IBM Center for The Business of Government and a Partner with IBM's Global Business Services. Frank is a career intelligence officer with 24 years experience in CIA's Senior Intelligence Service and the U.S. Marine Corps. During this time, Frank led a number of programs focused on developing innovative solutions and methodologies to measure and analyze mission performance. Frank co-founded Edge Consulting, a boutique consulting firm that achieved national recognition for pioneering work in the application of operations research methods and IT to quantify the value of intelligence.

engineer one of the largest breaches in history—the TJX heist. TJX was the largest theft of credit card data in U.S. history, totaling close to one and a half years' worth of T.J. Maxx credit card transactions, or about 94 million records in the U.S., Puerto Rico, and Canada.[10]

As cyber crime has evolved and forums for trading illicit goods and services have matured, the economy has diversified. This diversification has created demand for specialized services; seldom will only one individual create, fund, spread, and cash in on a criminal operation without such assistance. It has also created a taxonomy of recurring roles played by individuals in underground endeavors. These roles can be generalized into the following categories: leaders, technical elites, facilitators, and operators.

The Albert Gonzalez group had significant technical and facilitative connections with Eastern Europe, while the RBS WorldPay heist was perpetrated primarily by Moldovans, Estonians, and Russians. In fact, many of the large "carder" forums use (or used) Russian as the primary language, as indicated in Figure 2.[11]

However, as Figure 2 also shows, English is commonly found on these sites as well, and the role of the U.S. as host to infrastructure, operators, and targets in the cyber underground economy cannot be denied. Information from RSA's Anti-Fraud Command Center shows that the U.S. is the "top [phishing attack] hosting country—hosting 57 percent of attacks" and is also the top targeted country, with 37% of attack volume.[12]

Given the global nature of the Internet, this should not be surprising. Cyber crime is almost inherently a global phenomenon; just as traffic occurs on the World Wide Web, the cyber underground economy is worldwide as well. Global cyber criminals use the unique features of the Internet to increase their available targets, obscure their identity, and hamper police efforts.

Figure 3 shows the global extent of Zeus botnet command & control (C&C) servers (note that this likely represents more than one Zeus botnet and botnet operator).

How Does the Cyber Underground Economy Function?

Cyber crime in the traditional sense encompasses criminals motivated by greed and money. The lowest hanging fruit for cyber criminals is unknowing, uninformed users or

Figure 2. CarderPlanet.Com Website Front Page-partial (F-Secure)

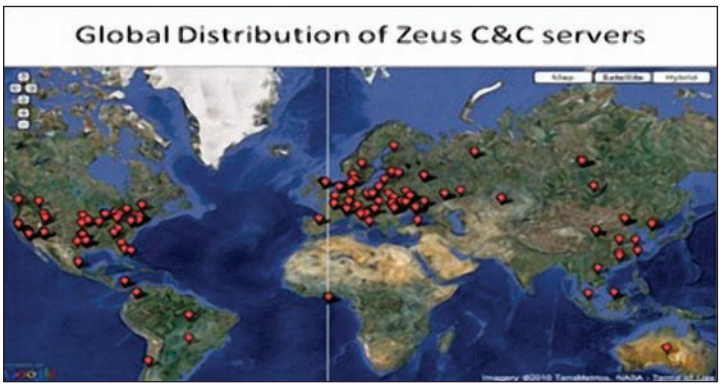

Figure 3. Global Zeus C&C Servers, Nov 2010 (Abuse.ch)

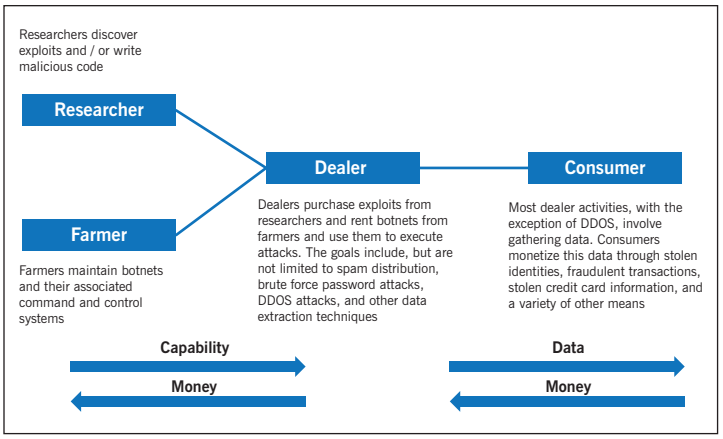

Figure 4. Information Theft and Resale Model (IBM)

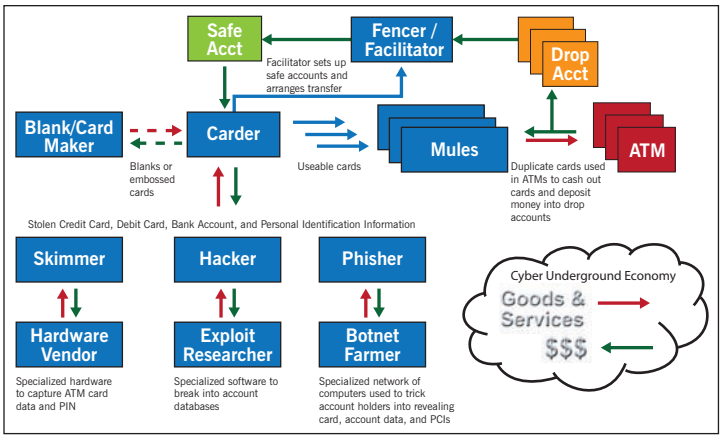

Figure 5. Example Carding Network (IBM)

consumers who fall victim to social engineering tricks, online fraud, or malicious e-mails. For a criminal, normal consumers offer little risk for decent gains. For example, spammers can potentially make up to US$8,000 per week, while botnet operators can make up to US$620,000 annually.[13]

Most of the cyber underground economy revolves around the theft, resale, and monetization of stolen information. There are many ways cyber criminals do this, but typically, a "dealer" will organize a campaign to illicitly obtain data of value, such as identity information, bank accounts, and debit or credit card information. The dealer enlists at least two other players in the underground economy.[14] The first is a technically sophisticated "researcher," someone who discovers security vulnerabilities or writes exploits the dealer can use to steal data.[15] Second, most operations require the services of a botnet farmer to send spam, host websites used in phishing attacks, host websites used in drive-by downloads, or provide any number of other services the dealer might use as an attack vector to obtain the desired data.[16] The dealer may employ other facilitators—for example, they may hire a spammer rather than conduct this part of the operation themselves.

From there, the dealer mounts the attack and collects data. The dealer then typically sells the data in bulk to operators or "consumers" who specialize in monetization through a variety of means: stealing money through ATMs with compromised debit cards, using stolen credit cards for fraudulent purchases, creating stolen identities, or performing any number of other forms of wire fraud. The whole process is depicted in Figure 4.

More specifically, carding networks refers to the individual and group associations that form to: 1) acquire 2) process 3) monetize and 4) distribute the proceeds from stolen payment card information. Carding networks are endemic of information theft and resale activities in the underground economy. Many Internet forums specialize in this particular activity, including a number of well-known examples, such as ShadowCrew and CarderPlanet. Figure 5 depicts the functions of a typical carding network.

Carding networks employ a variety of means to obtain compromised information. Some of the most popular include:

Phishing. In these operations, a spammer will send out e-mails that appear to come from a bank, a tax collection agency, or any other organization to which people will readily divulge financial information. These e-mails contain a link to a website that again appears official, but only serves as a front to collect the required data—in this case, name, debit card number, and PIN.

Network intrusion. A person with a wireless-enabled laptop breaks into a corporate network and downloads customer data, complete with card information. In the TJX case, Albert Gonzalez masterminded the compromise of over 45 million cards with this technique.[19]

ATM skimming. Vendors build specialized hardware that attaches directly to ATMs and gas pumps to capture the magnetic stripe and PIN from debit cards.

Malware. Vulnerability researchers identify exploits or write Trojans to capture the desired data. These tools use keystroke logging, form capture, screen capture—any technique the researcher can imagine to capture the data from the victim's computer or in transit. Computers become infected through drive-by downloads on websites, files contained in spam, or software vulnerabilities.[20]

The groups that capture the data will often sell it to another outfit that specializes in monetizing that data. Buyers and sellers come together on carding forums, where the data are often sold in bulk, with prices dependent on factors like the origin and verified value of the card. [21]

Most "cash out" operations utilize one or both of the following techniques:

Money mules. These individuals use duplicate ATM cards to take money directly from financial institutions. The mule takes a cut and places the rest in an account. From there, the money eventually reaches the data provider, often through a series of mules to disguise the transaction.

Reshippers. Reshippers use stolen account credentials from the data provider to purchase goods online, which are then shipped to a drop site. The reshipper picks up goods from the drop and ships them to the data provider in exchange for some percentage of the value of the item. These operations may employ a series of reshippers, again to obfuscate the transactions. [22]

An example of a typical carding forum is shown in Figure 6. This webpage is from "TheGrifters.net" carding forum, which was active from 2005-2006 after the ShadowCrew site was taken down by the U.S. Secret Service in Operation Firewall with the assistance of the young Albert Gonzalez.

Future Trends in the Cyber Underground Economy

It's clear that, without radical changes in the nature of the Internet, international cyber crime laws and enforcement, or security countermeasures, the cyber underground economy will continue to function and indeed may thrive. Prices of traditional goods and services seem to have steadily fallen since the early days of the economy and many now appear as commodities.

Although not authoritative, this information corroborates expert opinions that prices for payment card and personally identifiable information have fallen significantly.[23] This may be an indicator that the cyber underground economy is simply obeying laws of supply and demand, since, as seen in Figure 7, the availability (supply) of this information to criminals, by all accounts, has significantly increased over time.

The dropoff in compromised records in 2010 may be a result of the police takedown of Albert Gonzalez and his affiliates. If this is indeed the case, then there is hope that police action and cooperation can significantly impact the cyber underground economy. So far, however, there are no indications that the dropoff in records compromised in 2010 has resulted in increased prices on the cyber underground economy.

Unfortunately, the cyber underground has always reconstituted itself, even after very successful police operations. There are always those who evade the law and reconnect, in different forums or in private, with their partners in crime to attempt further scams. The vast and varied opportunities for the technologically savvy and morally bankrupt make this very likely to happen again in the future.

Technological advancements and changes in social behaviors as a result of technological innovation will continue to shape and drive criminal behavior. Advances in computing power, storage, and bandwidth serve as the foundation for an interconnected world of devices, networks, and social needs, making a ubiquitous computing environment a reality.

Figure 6. 'TheGrifters.Net' Carding Forum Webpage (Archive.org)

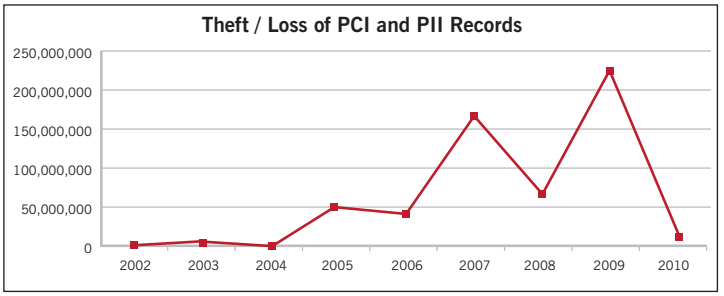

Figure 7. PCI/PII records compromised by theft or loss (2002-2010) (IBM/DataLossDB.org)

Trends in cloud computing, virtualization, expanded storage, and mobile computing continue to advance society's need for convenience, connectivity, and speed. At the distant end of the moral spectrum, these same trends enable criminal and corporate enterprises, and provide nation-states expanded access to lucrative information and a broader target set, whether for financial gain or economic, military, or political advantage.

New Thinking—New Solutions

In a recent Aspen Institute panel on cybersecurity, three cyber experts, including former NSA and CIA Director, General Michael V. Hayden, USAF (Ret.), emphasized that the cyber threat represents a fundamentally different security problem for which new thinking and solutions are required. Digital networks, which are becoming the central nervous systems for commercial, governmental, and societal enterprises worldwide, are attracting criminals ranging from cyber vandals to sophisticated organizations that specialize in cyber crime. The same technologies that increase the benefits of cyberspace, such as mobile devices and cloud computing, also present new vulnerabilities to criminal attacks.

These cyber criminals are fed by an underground economy. Perhaps government leaders' thinking should be unconventional in that, at least in the near term, as much or more emphasis is placed on the underground cyber economy and cyber crime as is placed on nation-states' capabilities and a potential cyber Pearl Harbor. Such thinking may lead to strategic benefits for our economy, and also government's ability to deter other problems in cyberspace, such as cyber attacks by nation-state sponsored groups. We hope that this information on the cyber underground economy will help public and private-sector leaders challenge their thinking about cyber priorities, and consider fundamentally new modalities for combating cyber crime and, specifically, the underground economy.

1 Independent of Shachtman's work, Gene Loughran led a team in 2010—with Ryan Moser and Scott Jung as primary contributors—that assessed implications of cyber underground economy to a national security mission.

2 http://en.wikipedia.org/wiki/The_414s

3 Fossl, Marc, et al. *Symantec Report on the Underground Economy from July 2007 to June 2008*. Symantec. 2008. PDF; http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf; http://www.gfi.com/security/pcifaqs.htm.

4 Fossl, Marc, et al. *Symantec Report on the Underground Economy from July 2007 to June 2008*. Symantec. 2008. PDF.

5 Paget, Francois. *Cybercrime and Hacktivism*. McAfee Labs. 2010. PDF.

6 *2009 Internet Crime Report*. Internet Crime Complain Center. 2009. 4. PDF.

7 DatalossDB.org. *Account Record Loss/Theft*. IBM Analysis. 2010.

8 http://mobile.eweek.com/c/a/Security/Web-Security-Report-Outlines-Structure-of-Cybercrime-Gangs/;http://mobile.eweek.com/c/a/Security/Inside-the-Russian-CyberUnderground-517933/

9 http://en.wikipedia.org/wiki/ShadowCrew

10 http://datalossdb.org/incidents/548-hack-exposes-94-million-credit-card-numbers-and-transaction-details

11 http://www.f-secure.com/weblog/archives/carderplanet_cc.htm

12 http://www.rsa.com/solutions/consumer_authentication/intelreport/11188_Online_Fraud_report_1110.pdf

13 Guerra, Peter. *How Economics and Information Security Affects Cyber Crime and What This Means in the Context of a Global Recession*. 2009 BlackHat Conference. 2009. 3. PDF.

14 http://www.securityweek.com/structure-crybercrime-organization-hackers-have-supply-chains-too

15 http://www.fastcompany.com/magazine/127/nexttech-fear-of-a-black-hat.html

16 Rajab,M.,Zarfoss,J.,"*A multifaceted approach to understanding the botnet phenomenon*," pp.41–52. 6th ACMSIGCOMM conference on Internet Measurement, SESSION: Security and Privacy, 2006.

17 Graham et al. Cyber Fraud TTPs, p. 22. 2009.

18 http://www.computerworld.com/s/article/97017/Secret_Service_busts_online_organized_crime_ring

19 Verizon Data Breach Investigations Report, p. 63. 2010.

20 Burgess, Christopher and Richard Power. *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century,* page 13. 2008.

21 Symantec Internet Security Threat Report, p.8. 2009

22 Graham et al. Cyber Fraud TTPs, p. 22. 2009.

23 http://mobile.eweek.com/c/a/Security/Web-Security-Report-Outlines-Structure-of-Cybercrime-Gangs/