Cyveillance
Minding your business on the Net

The Pioneer of
"Extra-Site"
e-Business Intelligence

To Catch a Cyber Thief

A White Paper

by Rick Grand
Senior e-Business Strategist
Cyveillance

September 11, 2000

NEW ECONOMY, OLD SCAMS

The Internet is transforming business, government and society. And why shouldn't it? Among other things, the Internet offers the ability to reach a global audience; to promote and sell products and services directly to the end user; to complete transactions instantly; and to experiment inexpensively with new marketing tactics and customer services. The capabilities and possibilities of the Internet continue to evolve and astound as the Internet grows to more than 2.1 billion total pages.[1] Yet, even as the Internet transforms business, government and society, one undesired element of the old economy remains: crime.

THE INTERNET: A CRIMINAL'S DELIGHT

Unfortunately, many of the features that make the Internet an ideal marketplace for business are also easily exploited for nefarious purposes. The perceived anonymity of the Internet and the diminutive start-up costs enable crooks to establish virtual street corners to conduct crime. These same low barriers to entry and exit permit criminals to evade detection by moving operations or closing them altogether at a moment's notice. Illegal outfits are also able to effectively mimic legitimate businesses by simply "borrowing" or replicating content from established ventures. Real-time or immediate payment capabilities offer instant payoff for the would-be felon. Additionally, online distribution remove the risk of an illegal transaction being witnessed by bystanders or law enforcement. The global reach of the Internet also complicates jurisdictional issues, sometimes impeding law enforcement efforts. And perhaps most alluring to cyber villains is the huge and ever-increasing number of potential victims that are instantly accessible, as worldwide Internet use surpasses 259 million people.[2] These elements contribute to the ease and appeal of the Internet as an ideal platform for perpetuating fraud or other criminal activity.

INTERNET CRIME COMES IN ALL SHAPES AND SIZES

Perhaps the most convincing testament to the popularity and effectiveness of the Internet as a mechanism to defraud and victimize is the vast array and volume of crime already occurring. The types of crime being uncovered range from the simple and obvious to the devious and complex. For instance, a man was recently sentenced to 14 months in prison for swindling eBay customers out of $37,000 by posting items for auction, selling them and then not delivering anything.[3] In another example, the state of New Jersey filed suit in March against eight online pharmacies for selling prescription medicines without a license.[4] Consumers merely had to complete a medical history form and pay a $65 fee to receive medicines—potentially at great risk to their health.

---

[1] *"Sizing the Internet,"* Cyveillance Inc., 7/10/00.

[2] Computer Industry Almanac Inc.

[3] *"US Targets Online Auction Fraud,"* E-Commerce Times, 2/15/00.

[4] *"U.S. States Target Illegal Online Pharmacies,"* E-Commerce Times, 3/31/00.

More recently, the U.S. Securities and Exchange Commission (SEC) shut down the Web site www.stockgeneration.com, a virtual stock exchange that allegedly defrauded over 800 individuals.[5] The SEC estimates that this pyramid scheme bilked millions from enterprising investors seeking to "double their money every month." In a more complex and unique case, the U.S. Federal Trade Commission (FTC) reported a scheme where visitors to the Web site www.sexygirls.com were prompted to download a purported "viewer program" to see computer images for free. Once downloaded, the consumer's computer was "hijacked" as the "viewer" program disconnected the computer from the local Internet access provider, dialed an international telephone number and reconnected the computer to a remote international site, accruing a $2 a minute charge until the consumer turned off the computer.[6] Appendix One provides a sampling of the different types of crime prevalent on the Internet. This list demonstrates that while new, Internet-specific crimes have emerged, much of the crime occurring on the Internet is comparable to illegal activities occurring in the offline world. As the technology evolves, the level of sophistication and variety of criminal activity will escalate proportionally.

THE IMPACT OF CYBER CRIME

The expansion of criminal activity to the Internet is occurring at an astounding rate. The government of the United Kingdom reported a 29% increase in Internet fraud and forgery over the past year.[7] According to the Industry Standard, one in five online shoppers has reportedly been a victim of fraud.[8] The U.S. Customs Service reports American companies are losing $200 billion a year to Internet piracy, and an FBI/Computer Security Institute study reported that over 90% of the responding organizations had detected cyber attacks, totaling over $266 million in estimated losses.[9, 10]

The direct and potential costs associated with cyber crime are staggering. Apart from the obvious financial impact Internet crime poses for individuals and organizations, other consequences may arise. Fundamentally, the rise in online criminal activity jeopardizes consumer trust and confidence in the Internet. Without the assurance of safety and security, the likelihood that consumers will conduct business transactions online is greatly diminished. In fact, a poll conducted by the Information Technology Association of America (ITAA) and Electronic Data Systems Corp. (EDS) found that 61% of Americans report they are less likely to do business on the Internet as a result of cyber crime.[11] Additionally, Internet crime threatens the public's confidence in the ability of government to protect citizens. The same ITAA/EDS poll reported that 62% of Americans believe not enough is being done to protect online consumers against crime.

---

5 *"Online Investors Lose Millions in Pyramid Scheme,"* E-Commerce Times, 6/16/00.

6 *"Fighting Consumer Fraud: New Tools of the Trade,"* Federal Trade Commission report, 4/98.

7 *"Government Reports Sharp Cyber-crime Rise,"* ZDNet UK, 1/20/00.

8 *"Who's Cheating Whom?"* The Industry Standard.

9 *"Cybercrooks Stealing $200 Billion Annually,"* E-Commerce Times, 10/6/99.

10 *"Study: Cybercrime Continues to Boom,"* E-Commerce Times, 3/22/00.

11 *"Net Users Worried Over Cybercrimes,"* Digitrends, 6/20/00.

THE CHALLENGES OF BATTLING ONLINE CRIME

To combat any type of Internet crime, the first challenge is to understand the extent of the problem. Fortunately for those charged with thwarting cyber crime, the majority of criminal activity aimed at the general masses is occurring on publicly accessible Web sites or news groups. But wrapping your arms around the entire Internet to locate problem sites in a thorough and methodical manner is easier said than done. Using popular search engines might help, but search engines have limited reach. In a recent study conducted by NEC Research Institute, AltaVista covered only 28 percent of the Internet, Northern Light about 20 percent and Excite about 14 percent. Search engines may assist in uncovering more popular sites; however, a terrorist boasting about committing an atrocious act is unlikely to take the steps necessary to be indexed by commercial search engines, which would make them easier for consumers and law enforcement agencies to locate.

Once the universe of sites engaging in a specified activity is defined, another hurdle is sifting through the sites, pinpointing and extracting those that meet certain criteria. For instance, efforts to uncover "pump and dump" stock schemes require filtering out legitimate investment sites from those offering a "sure thing" or "guaranteed returns." After isolating suspect sites, those sites must then be prioritized according to relevance or impact, so that resources can be deployed in the most efficient and expeditious manner. Clearly, sorting through this massive volume of information and prioritizing is tedious, time-consuming and often fruitless without the appropriate tools.

Finally, corporations and regulatory and law enforcement agencies must remain as vigilant and proactive about crime on the Internet as they are in the offline world. The ability to examine the information extracted from the Internet provides an essential means for staying ahead of the curve and uncovering emerging tools and techniques being employed to commit fraud or crime. Tracking and trending suspect sites, along with thorough analysis, will also assist in evaluating the success or impact of any enforcement actions undertaken, helping justify crime-fighting investments.

CRIME FIGHTING IN CYBERSPACE

As the tools and techniques utilized to engage in online criminal activity rapidly multiply, corporations and regulatory and law enforcement organizations have struggled to keep pace. For example, in response to a proliferation of unauthorized Web sites selling Mont Blanc products, Montblanc recently advised consumers to purchase their products only at authorized retail locations to guarantee authenticity.[12] Realistically, attempting to dissuade consumers from using the Internet or asking consumers to discern the legitimate sites from the bogus is a shortsighted remedy.

[12] *"Montblanc Fights Bogus Web Sales,"* Digitrends, 6/9/00.

In the U.S., the FBI, the SEC and the FTC, among others, have established Web sites for reporting Internet fraud. In the first three and a half days of service, the FBI's Internet Fraud Complaint Center (IFCC) logged 3,700 complaints. The SEC reports an average of 200 to 300 complaints registered daily to its online Enforcement Complaint Center.[13] These efforts will certainly create investigative leads, though the daunting volume of information can overwhelm and stretch the resources of any organization.

More proactive tools, such as organized Web surfing and consumer education efforts, are also being implemented. The SEC reportedly has a "Cyberforce" of 240 people who devote part of their time surfing for Internet fraud.[14] The FTC has utilized "surfer days" on which law enforcement personnel set aside a specific time to search the Internet for sites appearing to commit certain types of fraud. For example, a surfer day in October of 1997 focused on claims for products or services that promised to cure or prevent cancer, heart disease, AIDS, diabetes, arthritis, or multiple sclerosis. The surfers identified more than 400 Web sites and Usenet news groups that flaunted suspicious claims.[15]

While surfing will undoubtably uncover some criminal sites, sorting through and prioritizing those of greatest threat is time-consuming and laborious. Additionally, surfing requires massive amounts of time, thus either diverting employees from other assigned job responsibilities or necessitating the hiring of additional staff.

Consumer education efforts spearheaded by government agencies and consumer interest groups attempt to inform the public how to identify and recognize fraud. Typical of many government agencies, the Royal Canadian Mounted Police's Economic Crime Branch is attempting to increase public awareness of current online schemes, scams and criminal activity by posting information on its Web site. The success of education sites, however, hinges on the ability to reach the widest audience possible, a difficult task with limited marketing and advertising budgets of many government or public source entities.

NEW TOOLS OFFER A SOLUTION

To address these issues appropriately, new tools are required. One company, Cyveillance, is providing such a service—the company is the provider of "Extra-Site" e-Business Intelligence. The term "Extra-Site" is used by Cyveillance to convey the breadth of its proprietary NetSapien™ Technology, which mines and analyzes the Internet's billion of pages rather than tracking Web traffic and user data from within a specific corporate Web site. With the ability to scour millions of pages a day, NetSapien Technology mines the Internet in a thorough and methodical manner. NetSapien Technology is a Web-based tool with the ability to identify, filter, sort, and prioritize based upon customized needs. Additionally, it delivers

[13] *"The Web's Most Wanted,"* Business 2.0, 9/1/99.

[14] *"The Web's Most Wanted,"* Business 2.0, 9/1/99.

[15] *"Fighting Consumer Fraud: New Tools of the Trade,"* Federal Trade Commission report, 4/98.

only one page in a given domain, eliminating the possible redundancy of seeing many pages within the same domain. NetSapien Technology performs the investigative work quickly and inexpensively, freeing up the necessary resources within an organization to focus on enforcement action—the work for which they are trained.

The solutions delivered by Cyveillance are accessed via a password-protected Web site, enabling global organizations to securely share the same tools and information. Cyveillance archives all data, capturing and storing the evidence regardless of whether the status or content of a Web site changes.

In addition, Cyveillance's e-Business Strategy Center (eBSC) provides the hard-hitting analysis and tools necessary to recognize the trends, techniques and locations in which online crime is occurring. The eBSC also provides the analysis necessary to calculate an organization's return on investment in terms of actions taken and increased efficiency.

CONCLUSION: FIGHTING FIRE WITH FIRE

Cyber crooks have embraced the Internet as a productive mechanism for carrying out old tricks and trying some new ones. To thwart and deter cyber crime, corporations and regulatory and law enforcement agencies must similarly leverage new technologies. Current efforts to combat online crime are limited in their ability to effectively provide the greatest return within given resource constraints. Just as the new economy has achieved efficiencies by adopting new technologies, crime fighters must also harness those technologies to comprehensively and successfully respond to the growing threat posed by online crime.

ABOUT CYVEILLANCE

STRATEGIC SOLUTIONS

While some vendors in the e-Business Intelligence space today are focused on addressing one or two key issues, only Cyveillance takes a holistic approach-providing a complete solution to fuel executive decision-making and help companies run at maximum efficiency. Our Strategic Solutions address five key areas:

- Competitive Intelligence
- Brand Management
- Marketing Intelligence
- Partner Management
- Supplier Management

Because the Internet impacts every part of your organization-including your bottom-line-having a complete solution is a must. By tapping into Cyveillance's comprehensive "Extra-Site" e-Business Intelligence capabilities, your e-Business can begin firing on all cylinders.

And only Cyveillance offers NetSapien™ Technology, the most powerful business search and analysis tool available today. Our Strategic Solutions are built upon this unique, patent-pending technology and coupled with the expertise of our e-Business Strategy Center. Cyveillance solutions provide clients with strategic, competitive insights unavailable from any other vendor in the market place.

WE ALSO OFFER: INTELLECTUAL PROPERTY (IP) PROTECTION SOLUTIONS

If you're not sure who's capitalizing on the goodwill of your name or leveraging your valuable digital assets, Cyveillance's Intellectual Property Protection Solutions will identify and prioritize sites across the Internet that are using your intellectual property for their own financial gain. We have a track record and a technology designed to help you effectively monitor and protect your IP.

REGULATORY SOLUTIONS

The Internet has become the virtual street corner of the new millennium and many government entities and other organizations are now on the lookout for ways to proactively protect consumers. Cyveillance's Regulatory Solutions are designed to help government entities and other organizations seeking to proactively understand, manage and control cyber crime.

VALUE-ADDED CONSULTING

To complement our standard offerings, Cyveillance provides Value-Added Consulting designed to help you leverage and manage the intelligence you're already receiving from Cyveillance, give you the foundation you need to better understand the market and the competition, transform your business, cross the chasm or address the many other key corporate challenges you face today.

ABOUT THE AUTHOR

Rick Grand is a Senior e-Business Strategist in Cyveillance's e-Business Strategy Center. He has nine years of experience in the public and private sectors in public policy and program development, analysis, and implementation, project management, strategic planning, management consulting and Internet strategy. Prior to joining Cyveillance, he held positions with PricewaterhouseCoopers and the U.S. Department of Agriculture. He earned his Master of Business Administration from the Yale School of Management and holds a Bachelor of Arts degree from the University of Virginia.

Appendix One– Crimes Prevalent on the Internet

1. Online Fraud

A. Auctions

- Shilling* or self-bidding on items offered for auction
- Selling counterfeit or stolen goods
- Selling non-existent goods

B. Health

- Wonder drugs and remedies sold with false health claims
- Drugs sold without appropriate prescription or by unlicensed vendors
- Selling and importing drugs into areas imposing restrictions

C. Financial

- Securities fraud
- Insurance fraud
- Banking fraud
- Off-shore investment fraud
- Telemarketing fraud
- "Pump and dump" schemes
- Get-rich-quick schemes
- Money laundering
- Credit card fraud
- Cramming or charges for unexecuted phone calls
- Ponzi** and pyramid schemes
- Credit repair scams

2. Illegal Trafficking

- Drugs
- Firearms
- Police badges
- Stolen credit card numbers
- Child pornography
- Stolen or counterfeit goods
- Stolen passwords
- Repackaged expired or discarded products

3. Piracy and Grey Marketing

- Cybersquatting
- Stealing or misusing brands and logos
- Illegal distribution of software, movies and music
- Stealing proprietary content

4. Electronic Crimes

- Hacking instructions or other digital hacking tools
- Hijacking computers through downloaded software
- Identity theft
- Denial of service
- Launching viruses
- Pagejacking and mousetrapping

5. Terrorist Activity

- Planning, advocating or inciting criminal activity or violence
- Bomb building instructions
- Hate speech
- Boasting of criminal activity

*"Shilling" refers to bidding on an item you put up for auction to increase the price.

**A Ponzi scheme, named after Charles Ponzi who defrauded people in the 1920s using the method, involves getting people to invest in something for a guaranteed rate of return and using the money of later investors to pay off the earlier ones.