

## **Computer Addiction and Cyber Crime**

**Nick Nykodym**  
**The University of Toledo**

**Sonny Ariss**  
**The University of Toledo**

**Katarina Kurtz**  
**The University of Toledo**

*This research explores the relationship between computer addiction and cyber crime. There is evidence of computer addiction in medical settings, scholarly journals and legal proceedings. Reviewing the history of computer addiction has shown that computer addiction can be related to cyber crime. This paper will define computer addiction, show how various cyber crimes, especially those against businesses and organizations, can be motivated by computer addiction and propose further research on how managers can deal with cyber crime in a business, by recognizing addictive behaviors and computer addiction in their employees.*

### **HISTORY OF COMPUTER ADDICTION**

Computer addiction is an idea that has been in existence for years. Since the 1970s, avid computer programmers and hackers have been called “addicts” by both psychologists and the general public (Reed, 2002, p. 135). In 1976, Weizenbaum wrote about computer programmers who could sit and work at their computer terminals for twenty or thirty hours at a time. This behavior however, was viewed at the time as useful to technology and society.

Computers, once seen as huge government machines that only very knowledgeable people could use, transformed into user-friendly tools that could be used by the everyday person. It became more common to see computers in homes and businesses during the 1980s. This change meant more people were using computers, and more people were becoming addicted to computer use. The idea of computer addiction became more pervasive in the 80’s, and because of the social atmosphere of the time, there was widespread use of drug and addiction metaphors describing obsessive use of computers (Reed, 2002, p. 137). In fact, the PC is sometimes referred to as the “LSD of the 1980s” (Elmer-DeWitt, 1993, p. 63).

The Shotton studies on computer dependency in 1989 did nothing to discourage the idea of computer addiction. Shotton (1989) wrote that “in all instances where personal contact was made with people who worked with computers and computer users, there was belief in the occurrence of this syndrome (computer dependency)” (p. 20). Shotton mentions that many people felt that this dependency could also lead to negative consequences, such as academic and professional problems and decreased social interactions (Shotton, 1989, p. 20). Shotton’s analysis of computer dependent individuals found that they tend to be younger, unmarried men. Many were also first born children who had occupations within areas of science and technology (Shotton, 1989, p. 37). The result of these studies showed that computer dependency was a plausible syndrome and even began to show that profiling could be performed to show what kind of social and demographic influences nurture computer dependency.

During the 1990s, computer hacking became more widespread and resulted in the notion of hackers as “computer addicts.” In US courts, convicted hackers labeled as “addicts” saw increased rehabilitative therapy, computer use supervision and jail time. Computer hacker Kevin Mitnick’s history within the court system, shows how harsh punishments for computer crimes became during this time. In 1989, Mitnick was arrested for computer fraud and sentenced to one year in prison plus six months in an addiction rehabilitation program. At the time, this was the harshest sentence ever handed out by a court for this offence. Mitnick was released in 1990, only to be arrested again in 1995 for violating his probation by using computers. Mitnick was seen as an electronic terrorist and a dangerous individual, and he thus became the symbol of computer obsession gone wrong. For these reasons, it is not strange for Mitnick’s defense to be addiction and for his sentence to be so harsh. The Mitnick case introduced and legitimized the notion of clinical computer addiction to the US legal system (Reed, 2002, pp. 138-142).

The term Internet Addiction Disorder (IAD) was first coined by Dr. Ivan Goldberg in the late 1990s. The term was used to describe pathological obsessive computer use. Dr. Goldberg also used the terms webaholic and pathological computer use disorder. IAD is not currently listed as an addiction by the American Psychiatric Association (APA), but it is described under the category of Impulse Control Disorder (ICD) in the American Psychiatric Association (APA) Diagnostic and Statistical Manual, IV (Wieland, 2005, p. 154).

Other terms such as Pathological Internet Use (PIU) and Pathological Computer Use (PCU) are also used to describe computer addiction. These terms are used interchangeably with each other and with IAD. Though some experts argue that these syndromes are not truly mental diseases, proponents of computer addiction, notably those who run or work in clinics where patients are treated for these afflictions, claim that they are real diseases.

### **Diagnosing Computer Addiction**

There were an estimated 2.3 to 5.6 million addicted computer users in 1997 (Young, 1998, p. 27). In 2005, the estimate of addicted computer users increased from 11.3 to 18.9 (Kershaw, 2005). Fifteen signs of addiction, according to Internet/Computer Addiction Services in Redmond, Washington, are as follows:

1. Inability to predict the amount of time spent on the computer.
2. Failed attempts to control personal use for an extended period of time.
3. Having a sense of euphoria while on the computer.
4. Craving more computer time.
5. Neglecting family and friends.
6. Feeling restless, irritable and discontent when not on the computer.

7. Lying to employers and family about computer activity.
8. Problems with school or job performance, as a result of time spent on the computer.
9. Feeling of guilt, shame, anxiety or depression as a result of time spent on the computer.
10. Changes in sleep patterns.
11. Health problems such as carpal tunnel syndrome, eye strain, weight changes, backaches and chronic sleep deprivation.
12. Denying, rationalizing, and minimizing adverse consequences stemming from computer use.
13. Withdrawal from real-life hobbies and social interactions.
14. Obsessing about sexual acting out through the use of the Internet.
15. Creation of enhanced personae to find cyberlove or cybersex.

In addition to these symptoms, many experts also said that they see similar signs of withdrawal in computer addicts as in drug or alcohol addicts, symptoms such as profuse sweating, severe anxiety and paranoia (Kershaw, 2005). Furthermore, some patients are predisposed to becoming addicted to computers. Histories of psychological diseases or other types of addiction, such as gambling or drugs, make patients more susceptible to computer addiction (Wieland, 2005, p. 154). Computer addiction can also cause considerable development problems, including attention deficit disorder and other social issues, in young adults (Kershaw, 2005).

Computer addiction is a behavior-oriented addiction. "In behavior-oriented addiction, those who get hooked, are addicted to what they *do* and the *feelings* they experience when they are doing it" (Young, 1998, p. 17). Computers become a vehicle to compensate for other things lacking in a person's life such as relationships, solid marriages, strong and fulfilling careers or financial security. Computer addiction essentially becomes a catchall characterizing five main computer-related issues: cybersexual addiction, cyber relationship addiction, net compulsions (addiction to online gambling, stock trading, shopping, etc.), information overload (web surfing and database searching), and addiction to interactive computer games (Young, Pistner, O'Mara & Buchanan, 1999, p. 477, Wieland, 2005 p. 154).

The reasons men and women become addicted to the Internet are different. Men want to fulfill information glut, play explicit or aggressive games, and engage in cybersex. They seek control, power, influence and dominance. On the other hand, women look to the Internet as a source of friendship, romance and support (Wieland, 2005, p. 154). The types of experiences men gain from the Internet are more likely to become destructive, than the experiences women seek.

Denial is strong among sufferers of computer addiction. In 1998, Young noted the "one more minute syndrome." The name comes from the typical response given by computer addicts who are asked to get off the computer. These addicts become irritable when asked to get off because they lose their concentration and also the sense of euphoria they gain from their time online. Young noted that this rationalization of "one more minute," is very similar to an alcoholic who claims he or she will stop drinking after one drink.

Computer addicts can also create problems in a workplace environment. Employees who spend a lot of time on the computer can become easily irritable, causing increased arguments with coworkers and unfriendly work relationships. Increased time on the computer also results in decreased work activity and production (Beard, 2002, p. 6).

There is a growing number of treatment options for addicted computer users including behavioral therapy and inpatient rehabilitation centers. They use similar approaches in treating computer addiction as for other types of addiction, such as 12-step programs. Unfortunately, since IAD is not a currently recognized syndrome by the APA, insurance companies do not reimburse patients for these types of services. Patients either pay expenses out of pocket or therapists and treatment centers will bill for other problems, including impulse control disorders (Kershaw, 2005).

Unlike treatment for other addictions (drug, alcohol, etc.) which call for total abstinence, treatment for computer addiction is all about moderate, manageable use. The goal for computer addicts is to be able to use computers without becoming or remaining dependent on it as an escape from reality (Kershaw, 2005).

## **CRIME ADDICTION**

An increasing number of people are also starting to view crime as an addiction. There has been an upsurge in organizations modeled after Alcoholics Anonymous, which deal with criminal addiction. One group is Crime Addiction Anonymous out of Vancouver, Canada. It is “dedicated to the contentious premise that crime can be an illness as tenacious as dependency on alcohol or drugs” (MacQueen, 2004, p. 82). One of its members mentions his reasons for committing crimes as the power trip he receives and the fact that committing crimes is thrilling and fun.

Though some experts are reluctant to label this activity as “addiction,” many concede that crime can be caused by psychological needs. Psychologists have labeled criminals as “compulsive” or as being attracted by “the rush” (MacQueen, 2004, p. 83). Criminal motivation can also be based on psychological desires. Criminals may be seeking power, reassurance, trying to assert their power or seeking retaliation for past harms. In these cases, criminals are hoping to fulfill a psychological motive or need (Turvey, 2002, p. 310).

Opportunistic crime also exists. Evidence shows that some people commit crimes simply because they had the opportunity laid in front of them and took it (Turvey, 2002, p. 206). This shows a lack of restraint by these individuals, which can lead to further criminal activity.

Clinical psychologists have even tried to classify motives for crime in order to develop effective treatment for criminals to overcome their behaviors and prevent future criminal activity (Turvey, 2002, p. 307). Though there is no clinical term for crime addiction, psychologists still seem to be aware of the psychological element of crime and have a desire to treat criminals in order to cure them of their aspiration to commit crimes.

## **Computers and the Internet: Tools for Criminals**

In recent times, computers and the Internet have become very useful tools for criminals. All types of criminals, from hackers and spies to sexual predators and murderers, are able to use computers and the Internet to facilitate and ease the processes of their crimes. The Internet in particular is attractive to criminals for many reasons. 1) The Internet extends the reach of the criminal. Before the advent of the Internet, criminals were limited to committing crimes against people or businesses in their geographic locale. The Internet however, makes it possible for criminals to extend their reach all over the world. 2) The Internet helps criminals to more easily investigate potential victims. Criminals can alter their personality to obtain information directly from the potential victim, use the Internet to search for information on their potential victim, or

even hack into the victim's computer through the use of Trojan Horses or other spyware or viruses. 3) Criminals on the Internet feel safer committing their criminal acts because of their ability to conceal or alter their identities. This false sense of security can be their downfall, but at the same time it can be their vehicle to fuel fantasies, to fulfill information glut desires, or to feed a need for power (Turvey, 2002, pp. 549-550).

Internet criminals are motivated by a number of desires. Some are attracted to their crimes by the intellectual challenge, others are seeking power or attention and others, especially hackers, are motivated by a need to bolster their self-esteem. These motivations are rooted in psychological needs and can signify an obsessive or addictive personality (Turvey, 2002, pp. 552 & 555).

### **Computers and the Internet: Reason for Crime**

There is a general consensus among psychologists that past addictions, such as substance abuse or addiction to gambling, can lead to future addictive behaviors. Many computer addicts have a history of addiction. Addictive behavior breeds addiction. For these reasons, it is safe to say that computers are not only vehicles to commit crime, but computer addiction can become the reason for crime in general.

It is easy to see how computer addiction can lead to different types of crime, especially opportunistic crime. Individuals who spend a significant amount of time on their computers or the Internet, computer addicts, have many opportunities to commit crimes. These people may have never known that these criminal prospects existed before, but, by spending increased amounts of time on the Internet, have come to see a whole variety of opportunities laid out in front of them.

As it was previously mentioned, computer addiction can also lead to serious crimes against businesses. Computer addiction can cause increased irritability in employees and tension amongst coworkers. This can lead to increased employee turnover and training and human resources costs. Computer addiction also causes decreased productivity among workers, which can lead to significant reductions in profits for a company.

Computer addiction can also lead to information glut. A person can become so engrossed in finding out information and searching Internet databases, that he or she will start to overstep boundaries. This information craving can lead to hacking into company databases and even espionage. These criminals can be motivated by their addictions and by other psychological demands.

Computer addiction can lead to a false perception of reality. People feel that the Internet offers an escape from real life and allows them to remain invisible behind a barrier of anonymity. These feelings also give a computer addict a false sense of security, since he or she feels that there are no rules, and therefore no punishment, on the Internet. This fictitious existence makes it easy for individuals to feel no remorse for their crimes, and to believe there will be no reprimand for committing them.

### **Addiction and Profiling a Cyber Criminal**

There has been some research about how to profile cyber criminals. In 2005, Nykodym, Taylor and Vilela broke insider cyber crime down into four specific types and showed how the differences in the motives for the crimes, influence the kind of person who is willing and able to commit them. These categories of crime are espionage, sabotage, theft and personal abuse of an

organizational network. These categories and the profiling of the criminals will be explored in the following paragraphs.

The first type of crime, espionage, is generally committed by a spy planted in a company by one of its competitors. Since these spies are after top secret information, they are generally placed high in the hierarchy of the company so that they have more access to company records. Since managers are generally older individuals, spies will generally be at least thirty years and will be older if they assume positions of top management. Spies also want to blend in as much as possible in a company. For this reason, spies placed into organizations will reflect the race and culture structure of the particular company and will be very calm and reserved individuals. Spies also have a thorough understanding of computers and the IT area in a company in order to commit crimes and hide the evidence (Nykodym et al., 2005, p. 413).

Sabotage on the other hand, is generally caused by an individual for personal reasons. Saboteurs are similar to spies when it comes to knowledge of computers or IT, and are people who also have access to the company's network. Their motives however, are usually caused by a desire to get revenge on the company for a personal misfortune such as a missed promotion. These crimes can be committed while the criminal is still employed within the company or even after the criminal leaves or is fired by the company, as long as the criminal is still able to access or hack into the company network. Saboteurs are generally between the ages of twenty-five and forty, but have also been with the company long enough to have a complete knowledge of the company's network, especially its weaknesses (Nykodym et al., 2005, p. 413).

Thieves are also motivated by personal gain, but it is purely financial in nature. Thieves want to access valuable information from a company and use it for financial gain later. In 2005, Nykodym et al. showed that cyber crimes against a company valuing less than \$100,000 were generally committed by a man or woman who is between the ages of twenty to twenty-five years old and who is still in the lower hierarchy of the company. On the other hand, crimes costing a company between \$100,000 and \$1,000,000 are generally committed by a man between the ages of twenty-five and thirty-five. Crimes causing over \$1,000,000 of damage are caused by top management members, who are generally men over the age of thirty-five.

The last type of crime, abuse of a company's network, is the most common of the four categories. It can be caused by any individual in a company who uses the network for personal use such as reading the news, checking personal email, online gaming or gambling, etc. Though each case does not account for much loss, the sum of all loss of productivity within the company can be staggering. A person who commits this act against a company may "oppose supervisors, be non-conformant to rules and regularly break rules" (Nykodym et al., 2005, p. 414).

Managers at a company can fight insider cyber crime by setting up log-on accounts for employees, installing firewalls and limiting access to information based on job titles. Managers need to be observant of employee behavior and they also need to be forthright about the company's computer usage policies (Nykodym and Marsillac, 2007, pp. 8-9). In the future, managers may also be able to thwart cyber crime by recognizing addictive behaviors in an employee.

Though no research has been done to show how addictive personalities could be a determinate of cyber crime, it is easy to consider how addiction could cause cyber crime in an organization. It has already been shown how many people with computer addiction also have other addictions (e.g. gambling addiction), and how these addictions could easily lead to abuse of the company network. Addictive personalities could also lead to an increased desire to sabotage or steal for financial gain from a company. Further research needs to be done to show the extent

of addiction as a reason for crime and to see if programs set up by companies to help employees with addictive behaviors, especially addiction to computers, could minimize instances of insider cyber crime.

## **Conclusion**

Computer addiction, though not officially recognized by the APA as a disorder, nonetheless is commonly believed to be such a problem that treatment is needed to correct it. Symptoms are numerous, but one predisposing factor that can lead to computer addiction is a person with a history of other addictions. There is also growing support in favor of viewing crime as an addiction. A business setting can be a tempting atmosphere for an individual who has a problem with addictive behavior, since computer networks provide an easy vehicle through which cyber crime can be committed. Managers in businesses can fight back against cyber crime by learning to recognize addictive behavior and businesses in the future may be able to further thwart insider cyber crime by providing treatment programs for people suffering from computer addiction.

## **REFERENCES**

- Beard, K. (2002). Internet addiction: Current status and implication for employees. *Journal of Employment Counseling*, 39(1), 2-11.
- Elmer-DeWitt, Philip (1993, Feb 8). Cyberpunk. *Time Magazine*, 58-65.
- Kershaw, Sarah (2005, Dec. 1, late ed.). Hooked On the Web: Help is on the Way. *New York Times*, p. G1.
- MacQueen, Ken (2004, Dec. 27). Hooked on Crime. *Maclean's*, 82-83.
- Nykodym, Nick, & Erika L. Marsillac (2007, Mar. 4). The Managers Guide to Understanding, Detecting and Thwarting Computer Crime: An International Issue. Published in the proceedings of The National Business and Economic Society International meeting 2007.
- Nykodym, Nick, Robert Taylor, & Julia Vilela (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Report*, 408-414.
- Reed, Lori (2002). Governing (through) the Internet. *European Journal of Cultural Studies*, 5(2), 131-153.
- Shotton, Margaret (1989). *Computer Addiction? A Study of Computer Dependency*. London: Taylor & Francis.
- Turvey, Brent (2002). *Criminal Profiling*. London: Academic Press.
- Weizenbaum, Joseph (1976). *Computer Power and Human Reason*. New York: W.H. Freeman.
- Wieland, Diane M. (2005). Computer Addiction: Implications for Nursing Psychotherapy Practice. *Perspectives in Psychiatric Care*, 41, 153-161.

Young, K. (1998). *Caught in the net*. New York: Wiley.

Young, K., M. Pistner, J. O'Mara, & J. Buchanan (1999). Cyber disorders: The mental health concern for the new millennium. *CyberPsychology and Behavior* 2(5), 475-479.