

The Evolution of Computers and Crime: Complicating Security Practice

Rob D'Ovidio

Criminal Justice Program, Drexel University, Philadelphia, PA, U.S.A.

E-mail: rd64@drexel.edu

Security Journal (2007) 20, 45–49. doi:10.1057/palgrave.sj.8350045

Introduction

Technological developments in communications and information processing have, throughout history, been exploited for criminal purposes. As with the telegraph (Standage, 1998) and telephone (Shover *et al.*, 2003; D'Ovidio, 2005), computers and related networking technologies (Grabosky *et al.*, 2001; D'Ovidio and Doyle, 2003) have created new opportunities for crime and have affected the requisite capacity to commit criminal acts. News headlines such as “AT&T Hack Highlights Website Vulnerabilities” (Greenemeier, 2006) and “Cyber Crime Costs Business Billions” (Cowan, 2004) depict the criminal use of computers and bring to light some of the challenges computer crime present to the law enforcement and security communities.

Opportunities for computer crime have, undoubtedly, increased with continued advancements in computer and networking technologies, including the commercialization of the Internet. Law enforcement and security professionals need to, thus, remain vigilant in their assessment of new computer technologies to better understand the potential for victimization. The following essay discusses important developments in the history of the computer from the perspective of their impact on opportunities for crime and victimization.

Early computers and crime

In regulating the conduct related to the use of computers, the United States government currently defines a computer as “an electronic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device” (United States Computer Fraud and Abuse Act (e)(1), 1984). Such a definition takes into account the convergence of computing and telecommunication technologies. It reflects the information processing, storage, and transmission capabilities of today's computers. It covers traditional computing devices such as desktops, laptops, mainframes, servers, and routers, as well as newer computing devices such as personal digital assistants, smart phones, and portable media players.

Definitions of computer crime have evolved with the expanding role computers play in society and the increasing base of users. Early definitions described computer crime as a

type of white-collar crime that involved computer technology (Parker, 1976; Bequai, 1978). Such a description suggests a connection between those who commit computer crimes and their employment responsibilities (Sutherland, 1940).

The scarcity of computers prior to the introduction of the personal computer in 1975 by Altair limited the opportunity to commit a computer crime and the number of potential offenders. The high costs of mainframe, mini-, and super-computers prevented consumers from purchasing computers for home use and generally limited ownership to governments, large corporations, and research universities (Flamm, 1988; Campbell-Kelly and Aspray, 1996). Those with access to a computer through their employer or university had, consequently, the greatest opportunity to commit a computer crime (Parker, 1976; Whiteside, 1978). Criminal activity connected to these early computers generally involved unauthorized attempts to access proprietary data from within an organization and embezzlement or other large-scale institutional types of fraud (Bequai, 1987). Thus, security officials investigating early criminal activities involving computers, generally, had to look no further to identify the responsible party than those select employees or students who had computer privileges.

The number of potential offenders prior to the development of the personal computer was also limited by the technical skills needed to operate early computers. A requirement for the successful completion of any criminal activity is, according to Letkemann (1973), the knowledge and mechanical skill needed to operate associated tools and equipment. Letkemann's assertion is no less true for the offender who commits a computer crime as it is for the professional thief. The complexity of early computer-programming languages and interfaces required users to have technical skills that for the most part could be gained only by a small proportion of the population. The pool of potential offenders was, thus, further limited to only those insiders who possessed the requisite knowledge to bypass their authorized level of access and computer privileges.

Computer crime and the wide-spread adoption of the PC

The development of the personal computer, graphical user interface, and high-level programming languages¹ gave consumers a low-cost, easy-to-use solution to information processing and communication (Flamm, 1988; Campbell-Kelly and Aspray, 1996). Along with the commercialization of the Internet, these developments helped transform the computer from a tool used primarily by governments, large corporations, and research universities to a tool used by the public-at-large. In 1975, prior to the introduction of the first personal computer and the development of the graphical user interface, approximately 200,000 computers were operating in the United States (Parker, 1976). Since then, computer ownership has rapidly increased among public- and private-sector organizations, as well as within U.S. households. Data from October 1997 (Newburger, 1997), August 2000

¹ High-level programming languages (e.g. BASIC, FORTRAN, Pascal, Java, and Visual BASIC) use syntax that is closer to human language than do native machine languages. Native machine languages are read directly by a computer. A computer must convert, or compile, a program written in high-level language into machine language instructions before it can process the syntax. Programs converted into a native machine language contain only numbers and are, consequently, difficult for humans to interpret.

(Newburger, 2000), and October 2003 (Day *et al.*, 2005) Current Population Surveys highlight this influx of computer technology into the workplace, school, and home. Conducted monthly by the United States Census Bureau, the Current Population Survey gathers data on a variety of social and economic indicators from members of a nationally representative sample of U.S. households. The October 1997, August 2000, and October 2003 administrations of the Current Population Survey included supplemental questions about computer and Internet access in the workplace, school, and home. In October 1997, approximately 50 per cent of U.S. workers of 18 years and above used a computer at work. The U.S. workers who used a computer at work increased to 56.1 per cent in October 2003. Educational institutions in the U.S. also provided access to computer technology, with 80 per cent of students 3–17 years old reporting in August 2000 that they used a computer in school. Students who reported that they used a computer in school increased to 83.4 per cent in October 2003.

Among U.S. households, computer access has consistently increased since the mid-1980s. Approximately 62 per cent of U.S. households reported owning one or more computers in 2003, compared with 56.3 per cent in 2001, 51 per cent in 2000, 22.8 per cent in 1993, and 8.2 per cent in 1984 (Day *et al.*, 2005). Internet use in the U.S. is also on the rise. Internet use nearly doubled between 1997 and 2003, from 22.1 per cent to 59.5 per cent of the adult U.S. population, indicating that they used the Internet (Newburger, 2000; Day *et al.*, 2005).

The wide-spread adoption of computers and the Internet brought an increase in public-sector, private-sector, and consumer applications for these technologies. Computers have become general-purpose information-processing and communication machines that, among other things, mediate transactions in both the business-to-business and business-to-consumer markets, serve as commercial and personal communication devices, provide outlets for entertainment and leisure activities (e.g. video games, music, and movies), and enhance productivity through word-processing and analytical applications. The pervasiveness of computers and the Internet in the workplace, school, and home has increased both the opportunity to commit computer crime and the type of criminal activity that can be committed using a computer. Thus, past definitions that describe computer crime as a type of white-collar crime do not reflect the current extent of computer and Internet access throughout the United States and the full array of computer applications.

Today, computers continue to be both targets and instruments of crime (Parker, 1976; Charney, 1994). The wide-spread adoption of computers and the Internet and their ease-of-use have, however, moved computer crime beyond large-scale institutional types of fraud and attempts at access without authorization. Computer crime now includes, among other types of crime, copyright infringement, stalking, and consumer-oriented frauds, such as identity theft, check counterfeiting, and the unauthorized use of credit cards (D'Ovidio, 2005). Computers are also being used by adults to solicit children for sex and to produce, distribute, and store child pornography (Wolak *et al.*, 2003).

Besides being targets and instruments of crime, computers may also contain evidence of crimes that have occurred in the physical world. Offenders running illegal sports betting operations or brothels may, for example, use spreadsheets to record financial transactions and store client lists. Hurewitz and Lo (1993) offer a broad definition of computer crime that reflects the myriad of criminal acts one can commit with a computer. They define computer

crime as “any illegal act involving a computer that may be prosecuted under criminal law” (p. 496).

With the increase in the types of criminal activity one can commit involving computers and the number of people with the requisite skills needed to execute a computer crime comes an increase in the risk for personal and institutional victimization. Security professionals charged with protecting an organization now have to look beyond insiders for the pool of capable offenders when trying to identify the party responsible for a computer crime. Connectivity to the Internet for marketing, sales, and communication exposes an organization to attacks by geographically distant offenders and outsiders, or those who have no authorized access to an organization’s computing infrastructure.

Recent advances in computers and crime

The words mobile and ubiquitous are often used to describe the net-worked world of the future: a world that we are just beginning to get a glimpse of. Laptop computers, personal digital assistants, and smart phones allow for voice and data communication over third-generation wireless services and wireless-fidelity (i.e. Wi-Fi) networks. These wireless-enabled devices untether users from wired workstations and give them access to computer-processing capabilities, email, the Internet, corporate networks, productivity applications, music, movies, and games anytime and anywhere. Adults and children alike are quickly adopting these technologies, further increasing the potential and suitability for victimization from computer crime. In 2004, 66 per cent of American adults and 45 per cent of American youth, aged 12–17 years, reported that they own a cell phone (Lenhart *et al.*, 2005; Rainie and Keeter, 2006). In May 2004, 28 per cent of American adults indicated that they use a laptop with a wireless modem or a cell phone to connect to the Internet to surf the World-Wide Web and check email (Horrigan, 2004). Personal and organizational computer-security perimeters that in the past extended no further than the home and office, must now, consequently, be extended to follow the individual computer user wherever she may go. As more and more people use mobile devices to access computer infrastructures and information assets, security professionals will increasingly need to plan for contingencies that may arise in environments in which they have little or no familiarity and control.

Acknowledgements

I thank Bonnie Fisher and Martin Gill for inviting me to participate in this special issue of the *Security Journal*.

References

- Bequai, A. (1978) *Computer Crime*. Lexington: DC Heath and Company.
- Bequai, A. (1987) *Techno-Crimes: The Computerization of Crime and Terrorism*. Lexington: DC Heath and Company.
- Campbell-Kelly, M. and Aspray, W. (1996) *Computer: A History of the Information Machine*. New York: Basic Books.

- Cowan, R. (2004) Cyber Crime Costs Business Billions. *The Guardian*. Details of this can be obtained from http://www.guardian.co.uk/uk_news/story/0,3604,1155205,00.html, retrieved September 25, 2006.
- Charney, S. (1994) Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace. *Federal Bar News and Journal*. Vol. 41, No. 7, pp 489–494.
- D'Ovidio, R. (2005) *Crime.com: Does Crime have a New Face?* Dissertation Abstracts International, A6605, AAT 3176823.
- D'Ovidio, R. and Doyle, J. (2003) Cyberstalking: Understanding the Investigative Hurdles. *FBI Law Enforcement Bulletin*. Vol. 72, No. 3, pp 10–17.
- Day, J.C., Janus, A. and Davis, J. (2005) *Computers and Internet Use in the United States: 2003*. U.S. Census Bureau Publication No. P23-208 Washington, DC: United States Census Bureau.
- Flamm, K. (1988) *Creating the Computer: Government, Industry, and High Technology*. Washington, DC: Brookings Institution.
- Grabosky, P., Smith, R.G. and Dempsey, G. (2001) *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge: Cambridge University Press.
- Greenemeier, L. (2006) AT&T Hack Highlights Web Site Vulnerabilities. *Information Week*. Details of this can be obtained from <http://informationweek.com/news/showArticle.jhtml?articleID=192500500>, retrieved September 25, 2006.
- Horrigan, J. (2004) *American Adults are Wireless Ready: A PIP Data Memo*. Washington, DC: Pew Internet & American Life Project.
- Hurewitz, B.J. and Lo, A.M. (1993) Computer-Related Crimes. *American Criminal Law Review*. Vol. 30, pp 495–521.
- Lenhart, A., Madden, M. and Hitlin, P. (2005) *Teens and Technology: Youth are Leading the Transition to a Fully Wired and Mobile Nation*. Washington, DC: Pew Internet & American Life Project.
- Letkemann, P. (1973) *Crime as Work*. Englewood Cliffs: Prentice-Hall, Inc.
- Newburger, E.C. (1997) *Computers in the United States*. U.S. Census Bureau Publication No. 20-522. Washington, DC: United States Census Bureau.
- Newburger, E.C. (2000) *Home Computers and Internet Use in the United States: August 2000*. U.S. Census Bureau Publication No. 23-207. Washington, DC: United States Census Bureau.
- Parker, D.B. (1976) *Crime by Computer*. New York: Charles Scribner's Sons.
- Rainie, L. and Keeter, S. (2006) *How Americans Use Their Cell Phones*. Washington, DC: Pew Internet & American Life Project.
- Shover, N., Coffey, G.S. and Hobbs, D. (2003) Crime on the Line: Telemarketing and the Changing Nature of Professional Crime. *The British Journal of Criminology*. Vol. 43, No. 3, pp 489–505.
- Standage, T. (1998) *The Victorian Internet*. New York: Walker and Company.
- Sutherland, E.H. (1940) White-Collar Criminality. *American Sociological Review*. Vol. 5, No. 1, pp 1–12.
- Whiteside, T. (1978) *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. New York: Thomas Y. Crowell.
- Wolak, J., Mitchell, K. and Finkelhor, D. (2003) *Internet Crimes Against Minors: The Response of Law Enforcement*. Washington, DC: National Center for Missing & Exploited Children.