Computer crime

Computer crime, or **cybercrime**, is any crime that involves a computer and a network.The computer may have been used in the commission of a crime, or it may be the target. **Netcrime** is criminal exploitation of the Internet. Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

A report (sponsored by McAfee) estimates the annual damage to the global economy at $445 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.

Classification

Computer crime encompasses a broad range of activities.

Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;

- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.

A variety of internet scams many based on what is called Phishing as well as Social Engineering target direct to consumers, however, businesses are also susceptible to these scams.

Cyber terrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyber extortion

Cyberextortion is in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

An example of cyberextortion was the attack on Sony Pictures of 2014.

Cyber warfare

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.[12]

Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes requires the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.[13]

Crimes that use computer networks or devices to advance other ends include:

- Fraud and identity theft (although this increasingly uses malware, hacking and/or phishing, making it an example of both "computer as target" and "computer as tool" crime)
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware. Or, they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be legal.

Over 25 jurisdictions within the USA place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

Harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyberbullying, cyberstalking,hate crime, online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

There are instances where committing a crime, which involves the use of a computer, can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, Kramer was served an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3)[15] for his use of a cell phone to “persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct.” Kramer argued that this claim was insufficient because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, U.S. Sentencing Guidelines Manual states that the term computer "means an electronic, magnetic, 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 device."[16]

Connecticut was the first state to pass a statute making it a criminal offense to harass someone by computer. Michigan, Arizona, and Virginia have also passed laws banning harassment by electronic means.

Harassment as defined in the U.S. computer statutes is typically distinct from cyberbullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," while the latter need not involve anything of a sexual nature.

Threats

> Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate", that also applies for online or any type of network related threats in written text or speech. The US Supreme Court definition of "true threat" is "statements where the speaker means to

communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group".

Drug trafficking

"Drug traffickers are increasingly taking advantage of the Internet" according to cyber authorities and personnel. to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The deep web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again).

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

Documented cases

One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.

A hacking group called MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bell suffered losses of $370,000 alone.

In 1983, a nineteen-year-old UCLA student used his PC to break into a Defense Department international communications system.

Between 1995 and 1998 the Newscorp satellite pay to view encrypted SKY-TV service was hacked several times during an ongoing technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek re-runs in Germany; which was something which Newscorp did not have the copyright to allow.

On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and a copy of the virus spread via e-mail to other people.

In February 2000, an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high profile websites, including Yahoo!, Amazon.com, Dell, Inc.,E*TRADE, eBay, and CNN. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computerssending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors

charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.

The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad". It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with an individual activities earning up to $150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet.

On 2 March 2010, Spanish investigators arrested 3 in infection of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.

In August 2010 the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members, and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.

On March 1, 2011 at Lassiter High School, two students were accused of impersonation of a staff member via cybercrime, but both claimed they were uninvolved. The offense was made a felony in the Cobb County School District two months after the impersonation had happened. Shortly afterwards, the head of the LHS School Board said "The teacher just wouldn't do this at all". The case ended on May 9, and no evidence was found.

In June 2012 LinkedIn and eHarmony were attacked, compromising 65 million password hashes. 30,000 passwords were cracked and 1.5 million EHarmony passwords were posted online.

December 2012 Wells Fargo website experienced a denial of service attack. Potentially compromising 70 million customers and 8.5 million active viewers. Other banks thought to be compromised: Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.

In January 2012 Zappos.com experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been compromised.

April 23, 2013 saw the Associated Press' Twitter account's hacking to release a hoax tweet about fictional attacks in the White House that left President Obama injured. This erroneous tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, removal of $136 billion from S&P 500 index, and the temporary suspension of their Twitter account. The Dow Jones later restored its session gains.

Combating computer crime

Diffusion of Cybercrime

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Research Fellow at ESSEC ISIS), technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the cloud computing era, in order to spam one needed a dedicated server, skills in server management, network configuration and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack - brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.

Investigation

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide directive (applicable to all EU member states) states that all E-mail traffic should be retained for a minimum of 12 months.

Penalties

Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the internet or computers, even after they have been released from prison – though as computers and the internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyber offender behavior without resorting to total computer and/or Internet bans. These approaches involve restricting individuals to specific devices which are subject to computer monitoring and/or computer searches by probation and/or parole officers.