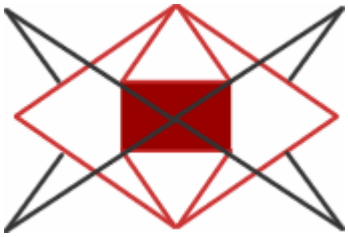
==========

|| Computer Crimes & Legal Implications||

==========



E-CQURITY

Author: Phuong D Nguyen, CISSP

COMPUTER CRIMES

GENERAL ISSUES

Nowadays, with the explosive growth of the Internet, proliferation of personal computers and easy access to the latest technology and high-end devices, life has changed to be so much more enjoyable and convenient than it was in past decades. The Internet revolution and advanced technology have opened up new possibilities with enormous provision for the enhancement and automation of living standards and business processes. No longer is there a need for people to go to the mall to buy things when they can just sit back, relax and start shopping through the Internet, using their personal computers. Neither is there a need to pay for a hefty phone bill for those expensive international phone calls, when e-mail can do the same thing — communicate with others — for much less. The technology brings everyone the benefits of automation and computing power, and in so doing, changes almost every aspect of life, either indirectly or directly. Crimes are not an exception either. Crimes would not be so sophisticated and diverse as they are today without the great assistance of technology in general. The technology perpetually changes the way crimes are usually committed. Criminals no longer need to walk out of their room to commit any unlawful acts; instead, they can do just about anything with their Internet-ready-PCs. Laundering money, transmitting viruses, manipulating stock markets and gaining unauthorized access to proprietary information are all examples of what high tech criminals are capable of doing these days. Any criminal activities that have the involvement or assistance of information technology, such as the Internet and high-end computers, are exclusively defined as *cybercrimes* or *computer crimes,* and they are further divided into three main categories:

- *Computer as tool*. Criminal activities that use and rely on computers to assist, and thereby, facilitate the crime. Examples of crimes in this category include financial fraud, telecommunication fraud, child pornography and so forth.
- *Computer as target*. Hacking related crimes usually reside here. Crimes in this category specifically aim at computers as well as the information stored on those systems, for example, denial of service or theft of proprietary information.
- *Computer is incidental*. The involvement of computers is incidental for the crimes and it is not essential as in the previous categories; for example, lists of stolen credit card numbers stored on the computers.

For clarification purposes, all discussions about computer crimes in this section will refer specifically to crimes of the first two categories — *Computer as target* and C*omputer as tool.*

Currently, more and more criminals have the ability to construct sophisticated attacks that outsmart the law and endanger the clients, or the industry as a whole, with much greater effects. Solutions to punish ordinary crimes in the real world cannot be used as a cure for combating crimes in virtual reality, where everything is in “0” and “1”. Computer crimes are constantly rising at full speed, as if nothing could ever stop them.

According to CERT (**C**omputer **E**mergency **R**esponse **T**eam), the number of security incidents that have been reported is growing at a rate of close to double every year, from

21,756 incidents reported in 2000 to a whopping 114,855 in 2003 (Q1-Q3). Moreover, in the latest *Computer Crime and Security Survey* released on June 10, 2004 by CSI (**C**omputer **S**ecurity **I**nstitute),it is reported that financial losses have dropped drastically from $201,797,340 in 2003 to $141,496,560 in 2004, according to 530 and 494 survey respondents, respectively.

However, in reality, not all security incidents are reported and not all the victims are aware of the intrusions; and therefore, the statistics from CERT and CSI can only reflect a tiny bit of the facts. If all the victims were aware of the intrusions and reported every single one to the authorities, then the real number of *reported* incidents as well as the financial losses would be much greater than one could ever imagine.

Based on those reported statistics from CERT and CSI; one could easily make a safe bet that easy access to the Internet and powerful personal computers helps crimes thrive at a faster pace and practically removes all inherent limitations. It is no longer an obligation for the threat agent, such as the attackers, to be physically at the scene to carry out bad deeds. The natural characteristics of the Internet and technology have changed all that. They have removed all obstacles and allowed the attackers to execute sophisticated transnational crimes without the need of physically leaving or entering a country. The Internet is, so to speak, like a mutual border of all countries where everyone can freely walk in, commit crimes, and walk out without the fear of being screened by the police or immigration officers. Inadvertently, this has formed a new genre of transnational crimes and criminals, which introduces law enforcement officials to countless investigations and jurisdiction issues and makes the process of tracing and apprehending the offenders very difficult, let alone prosecuting them. One of the main causes is due to the way the Internet handles and routes the traffic through many different countries and jurisdictions across the globe. In so doing, it conceals the location of where the attacks originated, and exacerbates the chances of tracing and prosecuting the offenders. On top of that, the attacks would allegedly fall outside the jurisdiction of the applicable laws if they were initiated from a country whose laws are not well enough to address the engaged activities as criminal activities.

Nevertheless, the Internet and technology are not the only things to blame for the rapid growth of cybercrimes. Difficulties in prosecuting and convicting computer criminals are also another factor encouraging other people to defy the laws and participate in unlawful activities. Perhaps the greatest challenge that the prosecutor has to face when dealing with cybercrimes is the handling of something intangible, such as evidence. Evidence pertaining to computer crimes is usually more vulnerable to alteration and forgery for the reason that they are in electronic form and intangible. The offenders can literally hinder legal proceedings, as well as intervene in investigative works of law enforcement officials by erasing or altering the relevant evidence. As a result, in order to prove the offenders guilty, it is the prosecutor's job to prove to the judge and juries the authenticity and integrity of the obtained evidence. Failure to do so results in inadmissibility of the evidence, and consequently, gives the offenders chances to avoid litigation.

Therefore, in order to address computer crime issues more effectively, several solutions have been proposed in the hope of punishing, and thereby deterring those who commit computer crimes. The solutions in question are the introduction of new laws and

high-tech law enforcement officials to control illegal activities on the Internet and bring the criminals to justice. The solutions indeed are able to solve parts of the problems; however, they also meet many challenges on the way.

The sudden rise of high-tech law enforcement officials and information system security professionals in recent years shows the high demands of stopping computer crimes from proliferating and bringing those who break the laws to justice. However, despite the formation of many security professionals and high-tech law enforcement officials all around the world, the volume of computer crimes has not ceased to increase as it should have. The criminals are getting smarter and more powerful with today's technology making computer crimes more sophisticated than ever. Yet law enforcement officials only do a little or nothing to prevent computer crimes from taking place, mainly because it is not their responsibility to do so and the lack of required skills makes it impossible for them to guess and catch up with the offenders' next move. From a more pragmatic perspective, focal functions of law enforcement are usually dealing with the aftermath of committed crimes, including prosecuting, punishing, and deterring the criminals.

Information system security professionals, on the other hand, are the ones who should be responsible for taking necessary steps to prevent computer crimes and mitigate the risks. Proactively propagating and raising security awareness and implementing strong security countermeasures are a few ways of what security professionals should be doing to help the industry prevent computer crimes. Security professionals and high-tech law enforcement officials both have different roles and tasks to accomplish; but for the benefits of the community, they normally work and assist one another to prevent, detect, and punish the wrongdoers.

The following are several canonical examples of computer crimes:

- *The Cuckoo's Egg.* After discovering a seventy-five cents discrepancy in a billing report, Clifford Stoll, a network administrator, uncovered and tracked down a German hacker who had been hacking into US military networks to gather classified information, and later on, selling it to the KGB. Clifford Stoll described his fascinating electronic pursuit in the book entitled *The Cuckoo's Egg*
- *Morris Worm.* In late 1998, a graduate student in computer science at Cornell University, Robert Tappan Morris, successfully created and released the first worm that had the capability to propagate itself across the Internet, by taking advantages of buffer overflow vulnerabilities found in various popular network daemons. Morris Worm is a leading example of the first successful prosecution of a computer crime case under the US Federal Law 18 U.S.C. § 1030.
- *Kevin Mitnick.* Kevin is by far the best known hacker in this world. With his extraordinary social engineering and computing skills, he has broken into many large and important computer and telephone networks to gain unauthorized access to proprietary information. In 1995, he was arrested by the FBI after breaking into the computer systems of a very well respected security researcher in San Diego, Tsutomu Shimomura.
- *Mafiaboy.* In early 2000, a 15-year-old kid known by the pseudonym Mafiaboy conducted a series of Distributed DoS attacks against several major commercial

websites, including Yahoo, Amazon, CNN, ZDNet, eBay and so forth. The attack disrupted normal operations of the websites and led the hacker to face a total of 64 charges related to illegal use of computer systems. According to the police investigation, Mafiaboy had rather an average knowledge of computing as well as hacking, but with easy access to the Internet and hacking tools, a novice hacker like Mafiaboy was able to construct a sophisticated attack that caused millions of dollars in damage. This attack is a great example of how technology can assist and facilitate a crime to occur with a greater impact.

LEGAL PERSPECTIVE — LAWS & PENALTY

CYBER SECURITY ENHANCEMENT ACT OF 2002

The legislation used for combating computer crimes is different from the one that you typically see everyday because the characteristics of computer crimes are not the same as of those real crimes in the real world. All the jurisdiction issues and uncoordinated efforts of many nations around the world has created a loophole that introduces a lot of difficulties in tracing, apprehending, and prosecuting computer hackers. The hackers virtually become untouchable, and that inadvertently sends the wrong message to the masses that current legal systems are not effective and strict enough. As a result, several computer-related crime laws have been exclusively enacted to address the differences and make the process of prosecuting and convicting computer criminals less painful. They also raise the penalty for those who violate the laws and commit computer crimes to a higher level. In fact, a strict statute that goes as far as putting criminal hackers behind bars for life already exists.

The Cyber Security Enhancement Act of 2002 is one of the strictest pieces of legislation to address computer related crimes and attempting to imprison any hackers, who use electronic means to endanger lives or cause serious injuries to others, for life. By penalizing the serious offenders with life imprisonment, the Cyber Security Enhancement Act of 2002 attempts to send a clear message to those hackers and would-be hackers that cybercrimes are just as serious as any other offense, and those who do not abide by the law will certainly be punished with no exception.

In addition to stringent penalties, the legislation also amends wiretap laws and allows government bodies to eavesdrop on any communication without having to obtain a court order first. Such actions are only appropriate if the offenses pose grave danger to national security or any entity in particular. Nevertheless, the legislation has sparked controversy between civil liberties groups and the authorities. On the one hand, the groups believe that the legislation is too intrusive that their privacy is crudely invaded; on the other hand, the authorities assert that the legislation is necessary for the protection of society.

OVERVIEW OF US FEDERAL LAWS

Enacted by Congress in 1984, the Counterfeit Access Device and Computer Fraud and Abuse Act was the first primary federal statute that could be used to prosecute computer-related criminal activity. The legislation, then, was very primitive in that it only addressed and punished those who endeavored to gain unauthorized access to classified

information on federal computers, or financial records and credit information on computers of large financial institutions.

Two years after the first enactment, Congress amended the statute in 1986 and broadened the scope of the legislation to cover crimes directed at “federal interest” computers and address three new additional offenses. Unfortunately, even after the amendment, the statute was still very narrow in defining computer crime and not yet covering computers of the private sector

Along with the rapid evolution of technology and the Internet, the Computer Fraud and Abuse Act of 1986 soon proved to be deficient in dealing with the foreseeable problems and new forms of computer crimes. In 1994, Congress amended the legislation and extended its capability to cover malicious code, including computer viruses, worms or destructive programs that alter, damage, and destroy data or information stored on computer systems. The amendment, which was also referred to as the Computer Abuse Amendment Acts of 1994, widened the scope of the previous legislation in 1986 by covering all computers used in interstate commerce, instead of covering just only “federal interest” computers.

In 1996, in order to keep up with the ever-changing technology and new instances of computer crimes, Congress once again further refined the effectiveness of the still-very-narrow federal statute by passing another amendment. Enacted as part of Public Law, the National Information Infrastructure Protection Act of 1996 significantly amended the Computer Fraud and Abuse Act, which is codified at Section 1030 in Title 18 of the United States Code (18 U.S.C § 1030). Perhaps one of the most remarkable changes of the amended Computer Fraud and Abuse Act was the wide coverage of computer-related criminal activity. The amended legislation not only covered crimes directed at “federal interest” computer systems but also broadened to cover “protected computers”, including computers used in foreign and interstate commerce, computers of the private sector or any computers connected to the Internet in general.

Before going any further to examine more federal statutes related to computer intrusions, you should first at least know how to interpret a standard federal statutory citation. A typical citation to a federal statute in the United States Code should contain the following elements:

- The title number of the Code
- The abbreviation for the Code (U.S.C)
- The section number within the title (abbreviated §)
- The year of the Code (publication year)

Hence, a federal statutory citation like 18 U.S.C § 1030 (1986) unambiguously refers to Section 1030 (Computer Fraud and Abuse Act) within Title 18 (Crimes and Criminals Procedures) of the 1986 edition of the United States Code. Normally, when citing a federal statute that is still in force, the year of the Code can be safely omitted without causing any confusion.

The list below presents some of the major federal statutes that can be used to address

and prosecute computer-related criminal activity:

- 18 U.S.C § 1029. Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C § 1030. Fraud and Related Activity in Connection with Computers
- 18 U.S.C § 1343. Fraud by wire, radio, or television
- 18 U.S.C § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C § 1831. Economic espionage
- 18 U.S.C § 2319. Criminal Infringement of a Copyright
- 18 U.S.C § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 U.S.C § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access
- 18 U.S.C § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information

Out of all those federal statutes introduced above, 18 U.S.C § 1029 and 18 U.S.C § 1030 are the two most important ones which are commonly used by prosecutors, judges, and juries to address computer-related crimes. Therefore, the next section will walk you through these pieces of legislation and examine them in more details.

SECTION 1029 OF TITLE 18 OF THE UNITED STATES CODE

In this information age, everything is virtually converted to digital and abstract form, which is obviously a big advantage when business processes increasingly require things to be done promptly and conveniently. Nevertheless, the advantage also brings along the associated risks. Intangible assets open up new opportunities for those criminals who want to perpetrate frauds but confined by vigorous physical security mechanisms. Implementation of security vault, surveillance camera, fireproof safe, or any other strong physical security measures is no longer an effective solution and is becoming a redundancy when it comes down to protecting intangible assets. Important assets, such as money, trade secrets, or business contracts, when stored in computerized format and exchanged over the wire are now a better target for technology literate criminals to perpetrate frauds, for the reason that they are not as well protected as in tangible form, and thus, can be easily counterfeited, altered, or stolen.

In response to the increasing numbers of computer-related fraudulent activities, Congress passed the Access Device Fraud Act which is also commonly known as 18 U.S.C § 1029 (Section 1029 of Title 18 of the United States Code). The federal statute strictly prohibits and criminalizes any activity that has the involvement of "counterfeit access devices" to perpetrate frauds. Exhibit 1-1 lists excerpts taken from the act. You should have a close look at the exhibit before going over to the brief analysis to see what the statute implies.

Exhibit 1-1. 18 U.S.C Section 1029

Fraud and related activity in connection with access devices

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10)without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

(c) Penalties. -

(1) Generally. - The punishment for an offense under subsection (a) of this section is -

(A) in the case of an offense that does not occur after a conviction for another offense under this section -

(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii)if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

Section 1029(a)(1) implies that whoever has the intention to defraud by knowingly producing, using, or trafficking in counterfeit access devices commits a federal offense. In other words, any activity involving access devices that are knowingly altered, counterfeited, designed, or duplicated for fraudulent purposes is strictly prohibited. The term “access device” is defined as any card, code, personal identification number, or instrument identifier that can be used to obtain anything of value. An example is credit cards duplicated without the owners’ consent by a dishonest bank teller for fraudulent gains.

***Penalty*:** Offense under Section 1029(a)(1) results in an appropriate fine and/or up to

10 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(2) states that it is an offense for whoever knowingly uses or traffics in unauthorized access devices to defraud and obtain anything of value $1000 or more during a one-year period. Unauthorized access devices refer to any devices which are stolen, revoked, or obtained for fraudulent purposes. One of the most typical examples of this offense is the traffic or trade of stolen credit card numbers between the hackers and the financial frauds.

***Penalty*:** Offense under Section 1029(a)(2) results in an appropriate fine and/or up to 10 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(3) primarily addresses the act of knowingly possessing fifteen or more counterfeit or unauthorized access devices to defraud. It constitutes a federal offense for anyone who is known to conduct and engage in such activities. A commonly seen example is when hackers break into an ecommerce website to steal credit cards, and thereby, either sell or use them for fraudulent gains. In early 2003, two major companies, Visa and Master Card, made headlines all around the world for opening up opportunities for hackers to gain unauthorized access to more than 5 million Visa and MasterCard credit card accounts in the US, but fortunately, none of which was used fraudulently.

***Penalty*:** Offense under Section 1029(a)(3) results in an appropriate fine and/or up to 10 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(4) provides that knowingly possessing or producing device-making equipment to defraud constitutes a federal offense. Device-making equipment refers to any equipment that can be used to create access devices, such as, magnetic card writer, card foil applicator, or card embossing machine. Ironically, these devices are, in fact, not very hard to find these days from many legitimate websites because they are usually sold under the claim of "for educational purposes *only*".

***Penalty*:** Offense under Section 1029(a)(4) results in an appropriate fine and/or up to 15 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(5) states that it is a federal offense for whoever knowingly uses an access device issued to another person to defraud and effect transactions to receive payment or anything of value $1000 or more during a one-year period. There's a similarity between this provision and the one under Subsection 1029(a)(2) in which both of them address and penalize the use of stolen credit card numbers to purchase merchandise from ecommerce sites such as high-end computer systems, or memberships to adult websites.

***Penalty*:** Offense under Section 1029(a)(5) results in an appropriate fine and/or up to 15 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(6) is a provision designed to address the act of knowingly soliciting a person for the purposes of offering an access device, or selling information that can be used to obtain an access device. Of course, engaging in such activity only

constitutes a federal offense when there is no authorization from the issuer of the access device and the actor must commit the act with the intent to defraud.

For instance, the provision under this subsection may apply to *phishing*, which is one of the most popular crimes arising in recent years. The offenders send an email under the name of a legitimate financial institution to falsely alert the victims about an emergency situation that requires the victims to provide their account numbers, password, personal identification numbers, or access code in order to "maintain" their accounts.

***Penalty*:** Offense under Section 1029(a)(6) results in an appropriate fine and/or up to 10 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(7) is more inclined to deal with fraud and related activity that has the involvement of telecommunications instruments. This provision prohibits and penalizes whoever engages in the act of knowingly using, distributing, or trafficking in modified telecommunications instruments, with the intention to defraud and obtain unauthorized use of telecommunications services. This would cover any activity related to *phreaking*, which refers the act of manipulating a telephone system, or network, in a way that would cause undesirable effects, such as, making free long-distance phone calls with the use of "red box" or "blue box" devices.

***Penalty*:** Offense under Section 1029(a)(7) results in an appropriate fine and/or up to 10 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(8) considers it is a federal offense for whoever has the intention to defraud by knowingly producing, using, or trafficking in a scanning receiver. According to subsection 1029(e)(8), the term "scanning receiver" is defined as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument". Therefore, offenses under this category are usually related to telecommunication frauds wherein the actors use a scanning receiver to intercept, or alter telecommunication instruments for the purposes of gaining unauthorized access to telecommunication services.

***Penalty*:** Offense under Section 1029(a)(8) results in an appropriate fine and/or up to 15 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(9) primarily designed to prohibit the act of using, producing, or trafficking in hardware or software whose its functionality is "to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument" so that such instrument can be used to obtain unauthorized telecommunications services. Knowingly conducting or engaging in such activity constitutes a federal offense under this subsection. The term "telecommunication identifying information" is defined as "electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument."

***Penalty*:** Offense under Section 1029(a)(9) results in an appropriate fine and/or up to

15 years in prison, or up to 20 years if repeat offense.

Subsection 1029(a)(10) states that knowingly causing or arranging for a person to present to the credit card system member or its agent, for records or transactions made by an access device is a federal offense, providing the offense must be committed with the intention to defraud and without authorization of the credit card system member.

***Penalty*:** Offense under Section 1029(a)(10) results in an appropriate fine and/or up to 10 years in prison, or up to 20 years if repeat offense.

SECTION 1030 OF TITLE 18 OF THE UNITED STATES CODE

As technology is gradually integrated into business processes, criminals no longer need weapons or transportation of any sort to facilitate crimes. Merely a decent computer with Internet connection can assist the criminals in executing sophisticated crimes, and causes just as much damage as any ordinary crime in the real world. As a result, Congress enacted the Computer Fraud and Abuse Act, or also formally referred as Title 18 U.S.C Section 1030, to address and prosecute computer-related criminal activity. Exhibit 1-2 is an excerpt from the act.

In order to make the analysis more understandable, Exhibit 1-2 only lists excerpts related to the constitution of federal offenses. The corresponding punishments to the offenses are included in another exhibit and will be discussed shortly.

Exhibit 1-2. 18 U.S.C Section 1030

Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) -

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

Section 1030(a)(1), in more simple terms, prohibits the act of knowingly accessing a computer without authorization or exceeding authorized access to obtain national defense or foreign relations, or classified information, and thereby, communicating, transmitting, or delivering the obtained information with the intent or reason to believe that the information can be used to injure the United States, or to the advantage of any foreign nation. Any person who deliberately engages in such activity or attempts to do so is subject to criminal prosecution under this provision.

It is worth noting that the provision does not prohibit the unauthorized transmission, control, or custody of the information, but it is the act of accessing a computer without authority, or in excess of authority, to obtain classified information that is prohibited.

Subsection 1030(a)(2), as you can see, designed to primarily protect the confidentiality of computer data by penalizing criminal activities related to obtaining unauthorized access to classified information. As in its original edition, the provision was only able to provide federal protection for financial records and credit information on federal and financial institution computers. However, the stipulation, then, was too narrow to be able

to keep up with the diversity and rapid growth of computer crimes. Consequently, Congress has redesigned subsection 1030(a)(2) and broadened its scope by insuring that it is punishable to misuse computers to obtain information held by the private sector rather than just government information such as financial records, or credit information.

Subsections 1030(a)(2)(a) and 1030(a)(2)(b) provide that whoever obtains confidential information from financial institutions, departments, or agencies of the United States by accessing a computer without authorization or exceeding authorized access commits a federal offense. In subsection 1030(a)(2)(c), "information" is further refined and widened to broadly cover information from any protected computer involved in foreign and interstate commerce or communication. The term "exceeds authorized access" clearly shows that the provision not only protects the confidentiality of information from outside breaches, but also prohibits the insider from abusing the given authority to subsequently gain access to the classified information, which he or she may not be entitled to obtain.

Nevertheless, it is important to see that "information" is not the main or only element that constitutes an offense and the provision itself does not punish the mere acquisition or reading of information, but it prohibits the act of knowingly accessing a computer without authorization, or exceeding authorized access, to obtain such information. For instance, when a hacker hacks into an ecommerce website to steal credit card numbers, it is the act of gaining unauthorized access to the computer to obtain credit card numbers that is prohibited under this provision, not just the taking or possession of those credit card numbers. Having control or custody of stolen credit card numbers is, however, normally prosecuted under Section 1029(a)(3) of Title 18 of the United States Code.

As defined in subsection 1030(e)(4)—not listed in the excerpt—the term "financial institution" means:

- an institution with deposits insured by the Federal Deposit Insurance Corporation;
- the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
- a credit union with accounts insured by the National Credit Union Administration;
- a member of the Federal home loan bank system and any home loan bank;
- any institution of the Farm Credit System under the Farm Credit Act of 1971;
- a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
- the Securities Investor Protection Corporation;
- a branch or agency of a foreign bank (as defined in the International Banking Act of 1978); and
- an organization operating under section 25 or 25(a) of the Federal Reserve Act.

Subsection 1030(a)(3) implies that it is an offense for whoever intentionally accesses a nonpublic computer of a department or agency of the United States, or a computer that is for the exclusive use of the United States government, without proper authorization. The provision also applies to the case where such a computer is not exclusively used by the United States government, but the conduct affects the use of the government's operation of that computer. Explaining this in other words, it is an offense to intentionally

access a nonpublic government computer without authorization. A "nonpublic" computer is any computer that is specifically designed for internal uses and it is not intended to be used or accessed by the public.

Subsection 1030(a)(3), whichever way you look at it, is not responsible to deal with either breach in confidentiality of information or intentionally misuses by the insider as in subsection 1030(a)(2). Indeed, the provision is designed to protect a nonpublic federal computer from outside breach and prosecute anyone who attempts to gain access to such computer without authorization, regardless of whether breach in confidentiality has or has not occurred. First violation of subsection 1030(a)(3) is always a misdemeanor.

Subsection 1030(a)(4) makes it a felony offense to further a fraud and obtain anything of value by knowingly accessing a protected computer without authorization, or exceeding authorization, with the intent to defraud. In short, the provision applies federal criminal sanctions when unauthorized use of the computer is momentous or exceeds $5,000 in any one-year period. Likewise, an exception from felony prosecution may apply to the case where the object of the fraud and the thing obtained is only the use of the computer and the value of that use is less than $5,000 in any one-year period. The term "protected computer" refers to any financial institution computer, government computer, or any computer involved in interstate or foreign commerce or communication.

Similar to subsection 1030(a)(2), the provision protects a computer from being abused by insiders and outsiders, such as hackers and disgruntled employees respectively. Under this provision, whoever attempts to access a protected computer and subsequently cause significant loss is held liable for felony offense, regardless of whether the actor is an authorized or unauthorized user. Although it is obvious that unauthorized user who knowingly accesses a protected computer without authorization should be punished, the punishment is also equally well applied to user who has authorized access to the computer and abuse such access to intentionally cause damage to the victim, or obtain things that they are not entitled to obtain.

Subsection 1030(a)(5)(a) has three different paragraphs addressing three different types of criminal conduct and consisting of two felony level sanctions and one misdemeanor.

The first one, subsection 1030(a)(5)(a)(i), primarily addresses the concerns regarding virus dissemination. The provision makes it a felony offense for anyone who knowingly causes the transmission of malicious code and intends to cause damage to a protected computer, regardless of whether they are outsiders, people who have no authorization, or insiders, those who abuse the granted authorization to intentionally cause damage. Although all other paragraphs of subsection 1030(a)(5)(a) exclude innocent insiders from being held liable for their actions, the provision of this paragraph is the only one that does not have such exclusion and will apply felony level sanctions to insiders who knowingly abuse their authority and intentionally cause damage.

In order to prosecute the actor for violation of subsection 1030(a)(5)(a)(i), the prosecutor must be able to prove that the actor knowingly causes the transmission of harmful code or programs *and* intends to cause damage. It is important that the actor must

knowingly participate in and violate both of the clauses, failure to show the actor's involvement in either one of those clauses makes it not possible to accuse for the actor for felony offense.

For example, the mere act of forwarding an email message and not knowing about the virus attachment will not hold the user liable for any crime or violation under subsection 1030(a)(5)(a), because the transmission of such harmful code is done unknowingly. In another example where the user knowingly forwards an email and the virus attached, the user would still not be held liable for felony offense under this provision if he or she did not intend to cause damage to the target recipients with such transmission. That happens when the user falsely believes that the virus is harmless and it only plays a bad song upon execution, while in fact, the virus aggressively destroys and alters computer data while playing along that bad song. As you can see, convicting the actor for felony offense under this provision can be a very difficult task in which the actor's intention in both the transmission and damage phases must be clearly shown.

Subsection 1030(a)(5)(a)(ii) and subsection 1030(a)(5)(a)(iii) are similar in that both of the provisions criminalize those who knowingly access a protected computer without authorization, and thereby, either recklessly or negligently cause damage. The term "without authorization" as mentioned in these provisions alludes to outsiders who do not have the authority to access a protected computer. In contrast with the provision of the first paragraph of subsection 1030(a)(5)(a) where criminal prosecution requires the damage to be committed intentionally by the actor, provisions of the last two paragraphs will punish whoever intentionally accesses a protected computer without authorization, regardless of whether the damage is caused intentionally, accidentally, or recklessly. Nevertheless, these provisions have different levels of punishment for different levels of damage and severity.

In subsection 1030(a)(5)(a)(ii), a felony level sanction is applied if the actor is an outsider who recklessly causes damage by intentionally accessing a protected computer without authorization. The provision clearly excludes insiders from such punishment because it is still a controversy matter whether authorized users should be held liable for reckless damage. Reckless as in today's computer environment could be the act of intentionally installing a strange software downloaded from the Internet without first checking it for virus or covert channels, and, imposing criminal sanctions or holding the user liable for such conduct are, obviously, inappropriate.

Subsection 1030(a)(5)(a)(iii) criminalizes the act of knowingly accessing a protected computer without authorization, and thereby, causing damage. At first, the difference between this provision and the one of subsection 1030(a)(5)(a)(ii) might not be noticeable where both of the provisions address and punish the intentional act of trespass. However, the difference lies in how different levels of damage warrant different levels of sanctions. As in subsection 1030(a)(5)(a)(ii), reckless damage caused by the trespassers warrants felony prosecutions, while within this provision, misdemeanor sanctions seem to be more appropriate to punish those who negligently or accidentally cause damage with their intentional act of unauthorized access.

The term "damage", which is repeatedly mentioned through all the three paragraphs

of subsection 1030(a)(5)(a), refers to “any impairment to the integrity or availability of data, a program, a system, or information”. The term is intentionally worded to be very broad and inclusive so that it is not limited to any specific act that can cause such impairment, preventing oversights of any types of harm. However, the broadness and inclusiveness of the term also sparks a lot of confusion when it comes down to defining what constitutes “damage”. Therefore, Congress has set several threshold harms to differentiate between significant and insignificant damage, and of course, to make the term “damage” more understandable. Those thresholds define damage as significant financial losses to one or more person aggregating at least $5,000 in value during any one-year period, impairment or potential impairment of medical treatment, physical injury to a person, threat to public health of safety, and affecting the computer’s use by or for a government entity.

Subsection 1030(a)(6) penalizes whoever traffics in any password or similar information that can be used to access a computer without authorization, providing that the offense is knowingly committed with the intent to defraud and the trafficking affects interstate or foreign commerce, or the affected computer is used by or for the Government of the United States. For instance, a hacker who boasts about his “elite” hacking skill by giving out a list of compromised usernames and passwords on www.whitehouse.gov clearly violates the provision.

Subsection 1030(a)(7) is a provision designed to address a new and emerging type of criminal conduct in today’s world, extortion with the involvement of a computer. In sum, the provision makes it illegal to cause the interstate or international transmission of threats directed against a protected computer, or network, with the intent to extort money or anything of value. Moreover, the provision covers threats to interfere in any way with the normal operation of the computer, such as preventing legitimate users from accessing the resources, or corrupting computer data. It does not really matter whether the threat is received by mail, e-mail, or a telephone call, but as long as it is a threat which against computers and their data, it is going to be covered by this provision.

In this information age, extortion with the use of powerful computer devices practically makes the old traditional way of extortion, such as kidnapping the target, or using unnecessary force, become obsolete. There was a case where a group of computer hackers blackmailed an ecommerce network for a large sum of money, and subsequently, threatened to perform DDoS (Distributed Denial of Service) attack to make the network in question unusable and unreachable if the owner disobeyed the request or failed to pay the ransom.

Exhibit 1-3 is an excerpt taken from 18 U.S.C §1030 which provides guidelines to punish those who commit offenses and violate the provisions.

Exhibit 1-3. 18 U.S.C Section 1030

Penalties

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for

another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if -

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(4)

(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

The analysis below is going to be divided into two parts. The first part provides you a list of corresponding punishments to first time offenders under Section 1030(a). A first time offense is an offense which does not occur after a conviction of another offense, or an attempt to commit an offense. The second part of this analysis lists the appropriate punishments for repeat offenses under Section 1030(a). A repeat offense is an offense which occurs after a conviction of another offense, or an attempt to commit an offense.

Punishment for first time offenses

Offense under subsection 1030(a)(1) constitutes a felony regardless of whether the amount of damage caused by such conduct is significant or insignificant. Offense under this provision warrants an appropriate fine and/or up to 10 years in prison.

Offense under subsection 1030(a)(2) can either result in a felony or a misdemeanor, depending on many other factors. Violation of subsection 1030(a)(2) can be a felony if the offense was committed for purposes of commercial advantage or private financial gain, or in furtherance of any unlawful act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000. However, if the offense does not meet any of those conditions, it is only a misdemeanor.

If the offense of subsection 1030(a)(2) is a felony offense, it warrants an appropriate fine and/or up to 5 years in prison.

If the offense of subsection 1030(a)(2) is a misdemeanor, it warrants an appropriate fine and/or up to 1 year in prison.

Offense under subsection 1030(a)(3) is always a misdemeanor if the offense does not occur after a conviction of another offense. A misdemeanor under subsection 1030(a)(3) warrants an appropriate fine and/or up to 1 year in prison.

Offense under subsection 1030(a)(4) warrants an appropriate fine and/or up to 5 years in prison. However, it is worth noting that if the amount of damage caused by the offense is not significant and does not exceed $5,000 in any one-year period, a felony level sanction may not be applicable to such conduct.

Offense under subsection 1030(a)(5)(a)(i) is a felony only if the offense reaches any one of the following significant thresholds:

- Significant financial losses to one or more person aggregating at least $5,000 in value during any one-year period;
- Impairment or potential impairment of medical treatment;
- Physical injury to a person;
- Threat to public health of safety; or
- Damage affecting the computer’s use by or for a government entity.

The term “loss” as mentioned above does not implicitly refer to a fixed amount of monetary loss of valuable things or assets. “Loss” can be aggregated and calculated from many factors, including the cost of responding to an offense, restoring the system, data, or program to a stable condition, losing customers, and “other consequential damages incurred because of the interruption of service”.

Similar to offense under subsection 1030(a)(5)(a)(i), offense under subsection 1030(a)-(5)(a)(ii) is a felony only when it meets several significant thresholds. Offense under this subsection warrants an appropriate fine and/or up to 5 years in prison.

Offense under subsection 1030(a)(5)(a)(iii) is a misdemeanor, it warrants an appropriate fine and/or up to 1 year in prison.

Offense under subsection 1030(a)(6) is a misdemeanor, it warrants an appropriate fine and/or up to 1 year in prison.

Offense under subsection 1030(a)(7) is a felony offense, it warrants an appropriate fine and/or up to 5 years in prison.

Punishment for repeat offenses

Repeat offense under subsection 1030(a)(1) warrants an appropriate fine and/or up to 20 years in prison.

Repeat offense under subsection 1030(a)(2) warrants an appropriate fine and/or up to 10 years in prison.

Repeat offense under subsection 1030(a)(3) warrants an appropriate fine and/or up to 10 years in prison.

Repeat offense under subsection 1030(a)(4) warrants an appropriate fine and/or up to 10 years in prison.

Repeat offense under subsection 1030(a)(5)(a)(i) warrants an appropriate fine and/or up to 20 years in prison.

Repeat offense under subsection 1030(a)(5)(a)(ii) warrants an appropriate fine and/or up to 20 years in prison.

Repeat offense under subsection 1030(a)(5)(a)(iii) warrants an appropriate fine and/or up to 10 years in prison.

Repeat offense under subsection 1030(a)(6) warrants an appropriate fine and/or up to 10 years in prison.

Repeat offense under subsection 1030(a)(7) warrants an appropriate fine and/or up to 10 years in prison.

Jurisdiction

The FBI (Federal Bureau of Investigation) have primary authority to investigate offenses under subsection 1030(a)(1) for any cases involving national defense, espionage, foreign relations, restricted data as defined in Atomic Energy Act of 1954. Subsection 1030(a)-(2)(c) and 1030(a)(7) also fall within the jurisdiction of the FBI.

The USSS (United States Secret Service) maintain concurrent jurisdiction over offenses under subsection 1030(a)(2)(a), 1030(a)(2)(b), 1030(a)(3), 1030(a)(4), 1030(a)(5), and 1030(a)(6).

For a more thorough explanation and analysis of Section 1030 of Title 18 of the United States Code, you should consider reading the official legislative analysis written by the Computer Crime and Intellectual Property Section of the United States Department of Justice at http://www.usdoj.gov/criminal/cybercrime/1030_anal.html.

REFERENCES

[1]. 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
http://www.usdoj.gov/criminal/cybercrime/1029NEW.htm

[2]. 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm

[3]. Legislative Analysis
http://www.usdoj.gov/criminal/cybercrime/1030_anal.html