(1) More and more, the operations of our businesses, governments, and financial institutions are controlled by information that exists only inside computer memories. Anyone clever enough to modify this information for his own purposes can reap substantial re wards. Even worse, a number of people who have done this and been caught at it have managed to get away without punishment.

(2) These facts have not been lost on criminals or would-be criminals. A recent Stanford Research Institute study of computer abuse was based on 160 case histories, which probably are just the proverbial tip of the iceberg. After all, we only know about the unsuccessful crimes. How many successful ones have gone undetected is anybody's guess.

(3) Here are a few areas in which computer criminals have found the pickings all too easy.

(4) Banking. All but the smallest banks now keep their accounts on computer files. Someone who knows how to change the numbers in the files can transfer funds at will. For instance, one programmer was caught having the computer transfer funds from other people's accounts to his wife's checking account. Often, tradition ally trained auditors don't know enough about the workings of computers to catch what is taking place right under their noses.

(5) Business. A company that uses computers extensively offers many opportunities to both dishonest employees and clever outsiders. For instance, a thief can have the computer ship the company's products to addresses of his own choosing. Or he can have it issue checks to him or his confederates for imaginary supplies or ser vices. People have been caught doing both.

(6) Credit Cards. There is a trend toward using cards similar to credit cards to gain access to funds through cash-dispensing terminals. Yet, in the past, organized crime has used stolen or counterfeit credit cards to finance its operations. Banks that offer after-hours or remote banking through cash-dispensing terminals may find themselves unwillingly subsidizing organized crime.

(7) Theft of Information. Much personal information about individuals is now stored in computer files. An unauthorized person with access to this information could use it for blackmail. Also, confidential information about a company's products or operations can be stolen and sold to unscrupulous competitors. (One attempt at the latter came to light when the competitor turned out to be scrupulous and turned in the people who were trying to sell him stolen information.)

(8) Software Theft. The software for a computer system is often more expensive than the hardware. Yet this expensive software is all too easy to copy. Crooked computer experts have devised a variety of tricks for getting these expensive programs printed out, punched on cards, recorded on tape, or otherwise delivered into their hands. This crime has even been perpetrated from remote terminals that access the computer over the telephone.

(9) Theft of Time-Sharing Services. When the public is given access to a system, some members of the public often discover how to use the system in unauthorized ways. For example, there are the "phone freakers" who avoid long distance telephone charges by sending over their phones control signals that are identical to those used by the telephone company.

(10) Since time-sharing systems often are accessible to anyone who dials the right telephone number, they are subject to the same kinds of manipulation.

(11) Of course, most systems use account numbers and passwords to restrict access to authorized users. But unauthorized persons have proved to be adept at obtaining this information and using it for their own benefit. For instance, when a police computer system was demonstrated to a school class, a precocious student noted the access codes being used; later, all the student's teachers turned up on a list of wanted criminals.

(12) Perfect Crimes. It's easy for computer crimes to go undetected if no one checks up on what the computer is doing. But even if the crime is detected, the criminal may walk away not only unpunished but with a glowing recommendation from his former employers.

(13) Of course, we have no statistics on crimes that go undetected. But it's unsettling to note how many of the crimes we do know about were detected by accident, not by systematic audits or other security procedures. The computer criminals who have been caught may have been the victims of uncommonly bad luck.

(14) For example, a certain keypunch operator complained of having to stay overtime to punch extra cards. Investigation revealed that the extra cards she was being asked to punch were for fraudulent transactions. In another case, disgruntled employees of the thief tipped off the company that was being robbed. An undercover narcotics agent stumbled on still another case. An employee was selling the company's merchandise on the side and using the computer to get it shipped to the buyers. While negotiating for LSD, the narcotics agent was offered a good deal on a stereo!

(15) Unlike other embezzlers, who must leave the country, commit suicide, or go to jail, computer criminals sometimes brazen it out, demanding not only that they not be prosecuted but also that they be given good recommendations and perhaps other benefits, such as severance pay. All too often, their demands have been met.

(16) Why? Because company executives are afraid of the bad publicity that would result if the public found out that their computer had been misused. They cringe at the thought of a criminal boasting in open court of how he juggled the most confidential records right under the noses of the company's executives, accountants, and security staff. And so another computer criminal departs with just the recommendations he needs to continue his exploits elsewhere.

(1) Все больше и больше, операций наших предприятий, правительства, и финансовых учреждений управляются информацией, которая существует только в компьютерной памяти. Каждый достаточно умный может модифицировать эту информацию для своих собственных целей, и могут снимать хороший урожай. И что хуже, целому ряду людей, которые совершили это и были пойманы при этом удалось остаться без наказания.

(2) Эти факты не были упущены преступниками или потенциальными преступниками. Последнее исследование Stanford'ского Научно-исследовательского Института злоумышленных действий на компьютере было основано на 160 случаях, которые вероятно являются только видимой частью айсберга. В конце концов, мы только знаем о неудачных преступлениях. Сколько успешных те, которые остались необнаруженными - никто не догадывается.

(3) Вот несколько областей, в которых компьютерные преступления были обнаружили слишком легко.

(4) Банковское дело. Все кроме самых маленьких банков теперь сохраняют свои учетные записи в компьютерных файлах. Кто-то, кто знает, как изменить числа в файлах, может перемещать средства по своему желанию. Например, один программист был пойман, перемещая средства с одних учетных записей на текущий счет его жены. Часто, традиционно обученные ревизоры не знают достаточно относительно работы компьютеров, чтобы ловить то, что имеет место прямо под их носами.

(5) Бизнес. Компании, которые широко используют компьютеры, предлагают много возможностей и нечестным сотрудникам и умным посторонним. Например, вор имея компьютер, может отправлять продукты компании по адресам на его усмотрение. Или может выпускать чеки, он или его сообщники для мнимых поставок или услуг. Люди сделавшие это было пойманы.

(6) Кредитные карточки. Есть направление по отношению к использованию карт подобным кредитным карточкам, чтобы получать доступ к средствам через банкоматы. Все же, в прошлом, организованные преступники использовали краденные или поддельные кредитные карты, для финансирования своих действий. Банки, которые предлагают услуги после работы (после закрытия магазинов) или дистанционные банковские операции через банкоматы, неохотно субсидируют организованных преступников.

(7) Кража информации. Теперь много персональной информации о человеке находится в компьютерных файлах. Человек с несанкционированным доступом к этой информации, может использовать ее для шантажа. Также, конфиденциальная информация относительно изделий компании или действий может быть украдена и продана недобросовестным конкурентам. (Одна последняя попытка была обнаружена, когда конкурент оказался добросовестным и появились люди, которые пытались продать ему украденную информацию).

(8) Кража программного обеспечения. Программное обеспечение для компьютерных систем часто более дорогое, чем аппаратные средства. Все же это дорогое программное обеспечение - слишком легко скопировать. Нечестные компьютерные эксперты разработали ряд хитростей для получения этих дорогих программ: распечатанных, на перфорированных картах, записанных на ленту или иным способом попавшая им в руки. Эти преступления даже совершают с дистанционных терминалов, которые имеют доступ к компьютеру через телефон.

(9) Воровство повременных услуг. Когда народу дают, доступ к системе, некоторые члены общества часто находят, как использовать систему неправомочными способами. Например, имеются "телефонные взломщики", которые избегают платы за междугородние звонки, они посылают сигналы управления телефонами, которые являются идентичными, тем, что используют телефонные компании.

(10) С тех пор как повременные услуги доступны каждому, тем кто сразу набирает телефонный номер, они подвергаются тем же типам обработки.

(11) Конечно, большинство систем используют учетные номера и пароли, чтобы ограничивать доступ незарегистрированным пользователям. Но недобросовестные лица оказались знатоками в получении этой информации и использовании ее для своих собственных целей. Например, когда защитная компьютерная система была продемонстрирована в школьном классе, развитой студент отмечал используемые коды доступа; позже, этих студентов учителя включали в список разыскиваемых преступников.

(12) Совершенные преступления. Компьютерным преступникам легко уходить необнаруженным, если никто не проверяет, кто работает на компьютере. Но даже если преступление было обнаружено, преступник может уйти прочь не только безнаказанно, но и с яркой рекомендацией от его прежних работодателей.

(13) Конечно, мы не имеем никакой статистики по преступлениям, которые были необнаруженными. Но обратите внимание, многие из преступлений, которые мы знаем были обнаружены случайно, а не систематическими ревизиями или другими процедурами безопасности. Компьютерные преступники, которые были пойманы, возможно, были жертвами необыкновенной неудачи.

(14) Например, один оператор клавишного перфоратора жаловался на необходимость остаться на сверхурочное время, чтобы делать дополнительные карты. Исследование показало, что дополнительные карты, которые он делал, были для мошеннических сделок. В другом случае, рассерженные соучастники вора предупреждали компанию, которую собирались грабить. В другом случае тайный агент спотыкнулся на наркотиках. Служащий продавал товары компании на стороне и использовал компьютер, чтобы отправить их покупателям. При ведении переговоров относительно LSD, агенту (наркотиков) предлагали много стерео (систем)!

(15) В отличие от других растратчиков, которые должны были покинуть страну, совершить самоубийство или идти в тюрьму, компьютерные преступники иногда нагло отрицают свою вину, требуя не только, чтобы они не обвинялись судом, но также, чтобы им давали хорошие рекомендации и возможно другие преимущества, как, например, выходное пособие. Все их требования слишком часто были удовлетворены.

(16) Почему? Поскольку руководство компаний боятся плохой рекламы, которая прекратила бы работу, если народ выяснил, что их компьютер неправильно использовался. Они съеживаются от мысли о преступнике, хвастающемся в открытом суде тем, как он манипулировал наиболее конфиденциальными отчетами прямо под носами руководителей компании, бухгалтеров, и штата защиты. Итак, компьютерный преступник уезжает с рекомендациями, которые ему нужны чтобы продолжать свои подвиги где-нибудь еще.