2007年英语四级复习资料（二十四） PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/252/2021_2022_2007_E5_B9_B4_E8_8B_B1_c83_252800.htm 最新英语四级模拟试卷《三》Part Ⅰ Writing(30 minutes)1. 表达你对Lawrence的想念之情；2. 介绍中国的春节；3. 邀请Lawrence和你们一起过春节。A Letter to LawrenceSeptember 23, 2005Dear Lawrence, Yours,Yuan ChaoPart Ⅱ Reading Comprehension (Skimming and Scanning、(15 minutes)For questions 8-10,complete the sentences with information given in the passage.Computer CrimeA computer crime is generally defined as one that involves the use of computers and software for illegal purposes. This doesn ’ t mean that all the crimes are new types of crime. On the contrary, many of these crimes, such as embezzlement of funds, the alteration of records, theft, vandalism, sabotage, and terrorism, can be committed without a computer. But with a computer, these offenses can be carried out more quickly and with less chance that the person responsible for the crime will be discovered. Computer crimes are on the rise and have been for the last twelve years. Just how much these computer crimes cost the American public is in dispute, but estimates range from ＄3 billion to ＄5 billion annually. Even the FBI, which attempts to keep track of the growth or decline of all kinds of crimes, is unable to say precisely how large a loss is involved. however, it estimates that the average take from a company hit by computer crime is ＄600,000. A number of reasons are given for the increase in computer crime: (A、 more computers in use and, thus, more people who are familiar with basic computer operation. (B、 more computers tied together in satellite and other datatransmission networks. and (C、 the easy access of microcomputers to huge mainframe data bases. The CriminalMovies and newspaper stories might lead us to believe that most computer crimes are committed by teenage “ hackers ” brilliant and basically good children who let their imagination and technical genius get them into trouble. But a realistic look at the crimes reveals that the offender is likely to be an employee of the firm against which the crime has been committed, i.e., an “ insider ” .Difficulty of Detection and PreventionGiven the kind of person who commits a computer crime and the environment in which the crime occurs, it is often difficult to detect who the criminal is. First of all, the crime may be so complex that months or years go by before anyone discovers it. Second, once the crime has been revealed, it is not easy to find a clear trail of evidence that leads back to the guilty party. After all, looking for “ weapons ” or fingerprints does not occur as it might in the investigation of more conventional crimes.Third, there are usually no witnesses to the computer crime, even though it may be taking place in a room filled with people. Who is to say if the person at the next terminal, calmly keying in data, is doing the company ’ s work or committing a criminal act?Fourth, not enough people in management and law enforcement know enough about computer technology to prevent the crimes. Authorities have to be familiar with the computer ’ s capabilities within a given situation to guard against its misuses. In some large cities, such as Los Angeles, police departments have set up specially trained computer crime units.But even when an offender is caught, the investigators, attorneys (律师、, judges, or juries may find the alleged crime too complicated and perplexing to handle. More attorneys are specializing in computer law and studying the computer ’ s potential for misuse. After a computer crime has been discovered, many companies do not report it or prosecute （起诉） the person responsible. A company may not announce the crime out of fear that the pubic will find out the weaknesses of its computer system and lose confidence in its organization. Banks, credit card companies, and investment firms are especially sensitive about revealing their vulnerabilities (脆弱性） because they rely heavily on customer trust.To avoid public attention, cautious companies will often settle cases of computer tampering out of court. And if cases do go to trial and the offenders are convicted, they may be punished only by a fine or light sentence because the judge or jury isn ’ t fully trained to understand the nature and seriousness of the crime.Not all companies are timid in apprehending computer criminals. For example, Connecticut General Life Insurance Company decided it had to get tough on violators. So when the company discovered that one of its computer technicians had embezzled ＄200,000 by entering false benefit claims, it presented it findings to the state ’ s attorney and aided in the prosecution of the technician. The technician was found guilty and sentenced to prison, not just for the computer misuse, but also for grand theft and insurance fraud. Connecticut General now has a policy of reporting all incidents of theft or fraud, no matter how small.1. The FBI knows exactly how large a loss is involved in computer crimes.2. It has become easy for microcomputer owners to use huge mainframe data bases.3. It is implied in the Paragraph 3 that most computer criminals are the employees of the concerned companies.4. Many companies dont report computer crimes because law procedures against computer crimes usually cost a lot of money.5. When computer crime takes place in a room filled with people, there are usually many witnesses to the crime.6.The passage is mainly about the increase of computer crimes in America and the difficulties in combating computer crimes.7. Computer crimes are on the rise because more cheap microcomputers are available.8. According to the passage, computer crimes has been on the rise for the last years.9. Connecticut General Life Insurance company is cited as of companies that took serious measures to fight against computer crimes.10. Banks, credit card companies, and investment firms are especially sensitive about revealing their vulnerabilities because they place too much reliance on .