Legal, Ethical, and Professional Aspects of Testing

14

Key Topics

Ethics
Law of Tort
Lawsuits
Professional Responsibility
Professional Negligence
Test Outsourcing
Software Licenses
Computer Crime
Hacking

14.1 Introduction

Ethics is a practical branch of philosophy that deals with moral questions such as what is right or wrong, and how a person should behave in a given situation in a complex world. Ethics explore what actions are right or wrong within a specific context or within a certain society and seek to find satisfactory answers to moral questions. The origin of the word "ethics" is from the Greek word ἠθικός, which means habit or custom.

There are various schools of ethics such as the *relativist* position (as defined by Protagoras), which argues that each person decides on what is right or wrong for them; *cultural relativism* argues that the particular society determines what is right or wrong based upon its cultural values; *deontological ethics* (as defined by Kant)

G. O'Regan, *Concise Guide to Software Testing*,
Undergraduate Topics in Computer Science,
https://doi.org/10.1007/978-3-030-28494-7_14

argues that there are moral laws to guide people in deciding what is right or wrong; and *utilitarianism* (as defined by Bentham) which argues that an action is right if its overall affect is to produce more happiness than unhappiness in society.

Professional ethics are a code of conduct that governs how members of a profession deal with each other and with third parties. A professional code of ethics expresses ideals of human behaviour, and it defines the fundamental principles of the organization and is an indication of its professionalism. Several organizations such as the Association Computing Machinery (ACM) and the British Computer Society (BCS) have developed a code of conduct for their members, and violations of the code by members are taken seriously and are subject to investigations and disciplinary procedures.

Business ethics define the core values of the business and are used to guide employee behaviour. Should an employee accept gifts from a supplier to a company as this could lead to a conflict of interest? A company may face ethical questions on the use of technology. For example, should the use of a new technology be restricted because people can use it for illegal or harmful actions as well as beneficial ones?

Consider mobile phone technology, which has transformed communication between people, and thus is highly beneficial to society. What about mobile phones with cameras? On the one hand, they provide useful functionality in combining a phone and a camera. On the other hand, they may be employed to take indiscreet photos without permission of others, which may then be placed on inappropriate sites. In other words, how can citizens be protected from inappropriate use of such technology?

14.2 Business Ethics

Business ethics (also called corporate ethics) are concerned with ethical principles and moral problems that arise in a business environment (Fig. 14.1). They refer to the core principles and values of the organization and apply throughout the organization. They guide individual employees in carrying out their roles and ethical issues include the rights and duties between a company and its employees, customers, and suppliers.

Many corporation and professional organizations have a written "*code of ethics*" that defines the professional standards expected of all employees in the company. All employees are expected to adhere to these values whenever they represent the company. The human resource function in a company plays an important role in promoting ethics and in putting internal HR policies in place relating to the ethical conduct of the employees, as well as addressing discrimination, sexual harassment, and ensuring that employees are treated appropriately (including cultural sensitivities in a multi-cultural business environment).

Companies are expected to behave ethically and not to exploit its workers. There was a case of employee exploitation at the Foxconn plant (an Apple supplier of the *i*Phone) in Shenzhen in China in 2006, where conditions at the plant were so

Fig. 14.1 Corrupt legislation. 1896. Public domain

dreadful (long hours, low pay, unreasonable workload, and crammed accommodation) that several employees committed suicide. The scandal raised questions on the extent to which a large corporation such as Apple should protect the safety and health of the factory workers of its suppliers. Further, given the profits that Apple makes from the *i*Phone, is it ethical for Apple to allow such workers to be exploited?

Today, the area of *corporate social responsibility* (CSR) has become applicable to the corporate world, and it requires the corporation to be an ethical and responsible citizen in the communities in which it operates (even at a cost to its profits). It is therefore reasonable to expect a responsible corporation to pay its fair share of tax and to refrain from using tax loopholes to avoid paying billions in taxes on international sales. Today, environment ethics has become topical, and it is concerned with the responsibility of business in protecting the environment in which it operates. It is reasonable to expect a responsible corporation to make the protection of the environment and sustainability part of its business practices.

Unethical business practices refer to those business actions that do not meet the standard of acceptable business operations, and they give the company a bad reputation. It may be that the entire business culture is corrupt or it may be result of the unethical actions of an employee. It is important that such practices be exposed, and this may place an employee in an ethical dilemma (i.e. the loyalty of the employee to the employer versus what is the right thing to do such as exposing an unethical practice).

Some accepted practices in the workplace might cause ethical concerns. For example, in many companies, it is normal for the employer to monitor email and Internet use to ensure that employees do not abuse it, and so there may be grounds for privacy concerns. On the one hand, the employer is paying the employee's salary and has a reasonable expectation that the employee does not abuse email and the Internet. On the other hand, the employee has reasonable rights of privacy provided computer resources are not abused.

The nature of privacy is relevant in the business models of several technology companies. For example, Google specializes in Internet-based services and products, and its many products include *Google Search* (the world's largest search engine); *Gmail* for email; and *Google Maps* (a Web mapping application that offers satellite images and street views). Google's products gather a lot of personal data and create revealing profiles of the users, which can then be used for commercial purposes.

A Google search leaves traces on both the computer and in records kept by Google, which has raised privacy concerns as such information may be obtained by a forensic examination of the computer, or in records obtained from Google or the Internet service providers (ISP). Gmail automatically scans the contents of emails to add context sensitive advertisements to them and to filter spam, which raises privacy concerns, as it means that all emails sent or received are scanned and read by some computer. Google has argued that the automated scanning of emails is done to enhance the user experience, as it provides customized search results, tailored advertisements, and the prevention of spam and viruses. Google's maps provide location information which may be used for targeted advertisements.

14.2.1 What Is Computer Ethics?

Computer ethics are a set of principles that guide the behaviour of individuals when using computer resources. Several ethical issues that may arise include intellectual property rights, privacy concerns, as well as the impacts of computer technology on wider society.

The Computer Ethics Institute (CEI) is an American organization that examines ethical issues that arise in the information technology field. It published the *ten commandments on computer ethics* (Table 14.1) in the early 1990s (Barquin 1992), which attempted to outline principles and standards of behaviour to guide people in the ethical use of computers.

The first commandment says that it is unethical to use a computer to harm another user (e.g. destroy their files or steal their personal data), or to write a program that on execution does so. That is, activities such as spamming, phishing, and cyberbullying are unethical. The second commandment is related and may be interpreted that malicious software and viruses that disrupt the functioning of computer systems are unethical. The third commandment says that it is unethical (with some exceptions such as dealing with cybercrime and international terrorism) to read another person's emails, files, and personal data, as this is an invasion of their privacy.

Table 14.1 Ten commandments on computer ethics

No.	Description
1	Thou shalt not use a computer to harm other people
2	Thou shalt not interfere with other people's computer work
3	Thou shalt not snoop around in other people's computer files
4	Thou shalt not use a computer to steal
5	Thou shalt not use a computer to bear false witness
6	Thou shalt not copy or use proprietary software for which you have not paid
7	Thou shalt not use other people's computer resources without authorization or proper compensation
8	Thou shalt not appropriate other people's intellectual output
9	Thou shalt think about the social consequences of the program you are writing or the system you are designing
10	Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans

The fourth commandment argues that the theft or leaking of confidential electronic personal information is unethical (computer technology has made it easier to steal personal information). The fifth commandment states that it is unethical to spread false or incorrect information (e.g. fake news or misinformation spread via email or social media). The sixth commandment states that it is unethical to obtain illegal copies of copyrighted software, as software is considered an artistic or literary work that is subject to copyright. All copies should be obtained legally.

The seventh commandment states that it is unethical to break into a computer system with another user's id and password (without their permission), or to gain unauthorized access to the data on another computer by hacking into the computer system. The eight commandment states that it is unethical to claim ownership of an intellectual creation that does not belong to you. (e.g. to claim ownership of a program that was written by another).

The ninth commandment states that it is important for companies and individuals to think about the social impacts of the software that is being created and to create software only if it is beneficial to society (i.e. it is unethical to create malicious software). The tenth commandment states that communication over computers and the Internet should be courteous, as well as showing respect for others (e.g. no abusive language or spreading false statements).

14.2.2 The Ethical Software Tester

Software testers are professionals and need to behave ethically at all times during testing. The ISTQB code of ethics for test professionals is based on the IEEE and ACM code of ethics and it states that:

- Certified software testers shall act consistently in the public interest
- They shall act in the best interests of their client and employer
- Certified software testers shall ensure that their deliverables meet the highest professional standards
- They shall maintain independence and integrity in professional judgments
- Certified software test managers and leaders shall promote an ethical approach to the management of software testing
- They shall advance the integrity and reputation of the profession
- Certified software testers shall be supportive of their colleagues and promote cooperation with software developers
- They shall participate in lifelong learning regarding the practice of their profession and promote an ethical approach to the practice of their profession.

14.3 Professional Responsibility of Software Engineers and Testers

Software engineering involves multi-person construction of multi-version programs. It requires the engineer to state precisely the requirements that the software product is to satisfy and to produce designs that will meet these requirements. It involves starting with a precise description of the problem to be solved; producing a design and validating the correctness of the design; finally, the implementation and testing are performed.

Parnas has argued that computer scientists need the right education to apply scientific and mathematical principles in their work. Software engineers need education on specification, design, turning designs into programs, software inspections and testing. This should enable the software engineer to produce well-structured programs using module decomposition and information hiding. He argues that "*software engineers have individual responsibilities as professionals*"[1]. They are responsible for designing and implementing high quality and reliable software that is safe to use. They are also accountable for their own decisions and actions[2] and have a responsibility to object to decisions that violate professional standards.

Professional engineers have a duty to their clients to ensure that they are solving the real problem of the client. They need to precisely state the problem before working on its solution. Engineers need to be honest about current capabilities

[1] The concept of accountability for actions dates back thousands of years. The ancient Babylonians employed a code of laws c. 1750 B.C. known as "The Hammarabi Code". This included a law that if a house collapsed and killed the owner then the builder of the house would be executed.

[2] However, it is unlikely that an individual programmer would be subject to litigation in the case of a flaw in a program causing damage or loss of life. Most software products are accompanied by a comprehensive disclaimer of responsibility for problems (rather than a guarantee of quality).

when asked to work on problems that have no appropriate technical solution, rather than accepting a contract for something that cannot be done.[3]

The *licensing of a professional engineer* provides confidence that the engineer has the right education, experience to build safe and reliable products. Otherwise, the profession gets a bad name because of poor work carried out by unqualified people. Professional engineers are required to follow rules of good practice and to object when rules are violated. The licensing of an engineer requires that the engineer completes an accepted engineering course and understands the professional responsibility of an engineer. The professional body is responsible for enforcing standards and certification. The term "*engineer*" is a title that is awarded on merit, but *it also places responsibilities on its holder*.

Engineers have a professional responsibility and are required to behave ethically with their clients. The membership of the professional engineering body requires the member to adhere to the code of ethics of the profession. The code of ethics[4] will detail the ethical behaviour and responsibilities including (Table 14.2).

14.3.1 ACM Code of Professional Conduct and Ethics

The Association of Computing Machinery (ACM) has defined a code of ethics and professional conduct for its members. The general obligations are detailed in Table 14.3.

14.4 Legal Aspects of Testing

Legal aspects of testing are concerned with the application of the legal system to the computing field. It includes intellectual property law including patents, copyright, trademarks, and trade secrets. Patents provide legal protection for intellectual ideas; copyright law protects the expression of an idea, and trademarks provide legal protection of names or symbols. There are potential legal impacts to an organization if the software has been inadequately tested, and if the quality of the testing is deemed to be negligent.

The problem of hacking is where a hacker uses his (or her) computer skills to gain unauthorized access to a computer system. We distinguish between ethical white hat hackers and malicious black hat hackers. Computer crime includes the unauthorized access of computer resources, the theft of personal information, cyber extortion, and denial of service attacks.

[3] Parnas applied this professional responsibility faithfully when he argued against the Strategic Defence Initiative (SDI), as he believed that the public (i.e. taxpayers) were being misled and that the goals of the project were not achievable.

[4] These are core values of most mature software companies and many companies today have a code of ethics that employees are required to adhere to.

Table 14.2 Professional responsibilities of software engineers and testers

No.	Responsibility
1.	Honesty and fairness in dealings with Clients
2.	Responsibility for actions
3.	Continuous learning to ensure appropriate knowledge to serve the client effectively

Table 14.3 ACM code of conduct (general obligations)

No.	Area	Description
1.	Contribute to society and human well-being	Computer professionals must strive to develop computer systems that will be used in socially responsible ways and have minimal negative consequences
2.	Avoid harm to others	Computer professionals must follow best practice to ensure that they develop high-quality systems that are safe for the public. The professional has a responsibility to report any signs of danger in the workplace that could result in serious damage or injury
3.	Be honest and trustworthy	The computer professional will give an honest account of their qualifications and any conflicts of interest. The professional will make accurate statement on the system and the system design and will exercise care in representing ACM
4.	Be fair and act not to discriminate	Computer professionals are required to ensure that there is no discrimination in the use of computer resources, and that equality, tolerance and respect for others are respected
5.	Respect property rights	The professional must not violate copyright or patent law, and only authorized copies of software should be made
6.	Respect intellectual property	Computer professionals are required to protect the integrity of intellectual property, and must not take credit for another person's ideas or work
7.	Respect the privacy of others	The professional must ensure that any personal information gathered for a specific purpose is not used for another purpose without the consent of the individuals. User data observed during normal system operation must be treated with the strictest confidentiality
8.	Respect confidentiality	The professional will respect all confidentiality obligations to employers, clients, and users

Software test tools are generally subject to a license, where a software license is a legal agreement between the copyright owner and the licensee that governs the use or distribution of software to the user. The two most common categories of software licenses that may be granted under copyright law are those for proprietary software and those for free open-source software.

Electronic commerce includes transactions to place an order, the acknowledgement of the order, the acceptance of the order where a legal contract now exists between both parties, and order fulfilment. We discuss the legal aspects of bespoke software development and test outsourcing, where a legal contract is prepared between the supplier and the customer. This will generally include a statement of work that stipulates the deliverables to be produced, and it may also include a service level agreement and an escrow agreement.

14.4.1 Legal Impacts of Failure

Software license agreements generally include limited warranties on the quality of the licensed software, and they often provide limited remedies to the customer when the software is defective. The software vendor typically promises that the software will conform to the software documentation for a specified period (the warranty period), and the software warranty generally excludes problems that are not caused by the software or are beyond the software vendor's control.

The customers are generally provided with limited remedies in the case of defective software (e.g. the replacement of the software with a corrected version, or termination of the user's right to use the defective software and a partial refund of the license fee). The payment of compensation for loss or damage is generally excluded in the software licensing agreement.

Software licensing agreements are generally accompanied by a comprehensive disclaimer that protects the software vendor from any liability (however, remote) that might result from the use of the software. It may include statements such as "*the software is provided* '*as is*', *and that the customers use the software at their own risk*".

A limited warranty and disclaimer limit the customer's rights and remedies if the licensed software is defective, and so the customer may need to consider how best to manage the associated risks. However, there are various lawsuits that could potentially be launched against a software provider and these are discussed in the next section.

14.4.2 Lawsuits and Professional Negligence

A lawsuit is a proceeding by a party (or several parties) against another party in a civil court. The basic principles of litigation are where the plaintiff sues another person(s) for being negligent, and the negligence of the defendant caused injury or damage to the property of the plaintiff. It involves proving in a court of law that:

- The defendant had a duty of care
- The defendant breached this duty of care
- The breach caused harm to the plaintiff or the property of the plaintiff.

The plaintiff is entitled to compensation of the full value of the injury or the damage to the property if the case is successfully proved. Further, if there is clear evidence that the defendant acted maliciously or fraudulently then punitive damages may be awarded to the plaintiff to punish the defendant. Punitive damages are generally awarded in a small percentage of lawsuits, and they may be appealed to a higher court.

There are several types of lawsuit that may be brought against a software company (the defendant) including (Table 14.4).

14.4.3 The Law of Tort and Testing

The *law of tort* refers to a civil wrong where one party (the *defendant*) is held accountable for their actions (by the *plaintiff*). There are several actions that the defendant could be held accountable, e.g. negligence, trespass, misstatement, product liability, defamation, and so on. For example, the defendant may be accused of negligence and a breach of his duty of care, where damage that was reasonably foreseeable was caused by negligence.

The impact of a flaw in software may be catastrophic, and so a software development organization must take all reasonable precautions to prevent the occurrence of defects (as otherwise it may be sued for negligence). This is especially true in the safety-critical domain, where defects could cause major damage or even loss of life. Reasonable precautions consist of having appropriate software

Table 14.4 Types of lawsuits

Type	Description
Criminal	This type of lawsuit is brought by the state against the software company (or developers or testers) for committing a criminal act (e.g. tampering with a computer or loading a virus onto a computer)
Tort	This type of lawsuit is brought by an individual(s) against a company/developers for committing some wrong to you or your computer (e.g. releasing a virus onto your computer)
Negligence	The company has a duty of care to take reasonable measures to make the product safe, so that there are no personal injuries or damage to property
Malpractice	This is where the quality of service is judged against a professional standard and deemed to be negligent, with mistakes made in the delivery of the service that would not be made by an ordinary professional in the field
Strict liability	A product defect caused a personal injury or damage to property, and the burden of proof required is to demonstrate that the program was defective and that the defect caused the accident (e.g. failure of program controlling breaks in a car)
Fraud	The company made a statement of fact to you when it knew that the statement was false (and where you relied on the statement to make an economic decision such as buying a defective product)
Regulatory	The regulatory sector (e.g. FDA) places requirements on how software should be developed and tested so that it is safe for the public to use
Breach of contract	A software contract specifies the obligations that both parties have to each other (as well as implied terms such as implied warranty)

engineering practices in place to allow the organization to consistently produce high-quality software.

A quality management system indicates that the organization takes software quality seriously and has a sound software development process in place that serves the needs of the organization and its customers. Modem quality assurance systems include processes for software inspections, testing, quality audits, customer satisfaction, software development, project planning, etc.

The organization will require evidence or records to prove that the quality management system is in place, and that it is appropriate for the organization, and that it is fully operational within the organization. This generally requires records and an audit trail of the various quality activities to be maintained. The records enable the organization to prepare a legal defence to show that it took all reasonable precautions in software development, especially if a customer decides to take legal action for negligence against the software provider following a serious problem in the software at the customer site.

The presence of records may be used to indicate that all reasonable steps were taken, and the records typically include lists of all the deliverables in the project; minutes of project meetings; records of reviews of requirements, design, and software code, records of test plans and test results; and so on.

14.5 Legal Aspects of Test Outsourcing

Test outsourcing and bespoke software development have become popular in the software engineering field. Test outsourcing is where the testing is outsourced to an independent external organization. Bespoke (or custom) software is software that is developed for a specific customer or organization, and it needs to satisfy the defined customer requirements. The organization will need to be rigorous in its selection of the appropriate supplier (as discussed in Chap. 8), as it is essential that the supplier selected has the capability of delivering high quality and reliable software on time and on budget.

This means that the capability of the supplier is clearly understood and the associated risks are known prior to selection. The selection is based on objective criteria such as cost, the approach, the ability of the supplier to deliver the required solution, the supplier capability, and while cost is an important criterion, and it is just one among several other important factors.

Once the selection of the supplier is finalized a legal agreement is drawn up between the contractor and supplier, which states the terms and condition of the contract, as well as the statement of work (Fig. 14.2). The *statement of work* (SOW) details the work to be carried out, the deliverables to be produced, when they will be produced, the personnel involved their roles and responsibilities, any training to be provided, and the standards to be followed. The agreement will need to be signed by both parties and may (depending on the type of agreement) include:

Fig. 14.2 Legal contract. Creative Commons

– Legal contract
– Statement of work
– Implementation plan
– Training plan
– User guides and manuals
– Customer support to be provided
– Service level agreement
– Escrow agreement
– Warranty period.

A *service level agreement* (SLA) is an agreement between the customer and service provider, which specifies the service that the customer will receive as well as the response time to customer issues and problems. It will also detail the penalties should the service performance fall below the defined levels.

An *escrow agreement* is an agreement made between two parties where an independent trusted third party acts as an intermediary between both parties. The intermediary receives money from one party and sends it to the other party when contractual obligations are satisfied. Under an escrow agreement the trusted third party may also hold documents and source code.

Occasionally, it will be just the testing part of a project that is outsourced, and test outsourcing is concerned with the selection and management of an appropriate supplier to perform the testing. It is essential that the selected test organization is capable of carrying out the required testing to the defined quality standard, as well as being capable of completing the testing within the budget and schedule constraints.

The legal contract specifies the obligations of the supplier and should the supplier fail to honour its commitments it may well be in breach of contract. This means that the binding agreement has not been honoured, and there may be a need to seek legal remedy if a *material* breach of the contract has occurred. The first step is dialogue between both parties with the objective of finding a reasonable resolution, but if both parties are unable to agree a way forward the first party may seek a legal remedy in a civil court.

14.6 Licenses for Test Tools

Testers often employ dedicated test tools for various parts of the test process, and the use of tools is generally subject to a licensing agreement. The tools may be developed in-house, but it is more common to employ proprietary tools or open-source tools. A software license is a legal agreement between the copyright owner and the licensee, which governs the use or distribution of software to the user (licensee). Computer software code is protected under copyright law in most countries, and a typical software license grants the user permission to make one or more copies of the software, where the copyright owner retains exclusive rights to the software under copyright law.

The two most common categories of software licenses that may be granted under copyright law are those for *proprietary software* and those for *free open-source software* (FOSS). The rights granted to the licensee are quite different for each of these categories, where the user has the right to copy, modify, and distribute (under the same license) software that has been supplied under an open-source license, whereas proprietary software typically does not grant these rights to the user.

The *licensing of proprietary software* typically gives the owner of a copy of the software the right to use it (including the rights to make copies for archival purposes). The software may be accompanied with an end-user license agreement (EULA) that may place further restrictions on the rights of the user. There may be restrictions on the ownership of the copies made, and on the number of installations allowed under the term of the distribution. The ownership of the copy of the software often remains with the copyright owner, and the end user must accept the license agreement to use the software.

The most common licensing model is per single user, and the customer may purchase a certain number of licenses over a fixed period. Another model employed is the license per server model (for a site license), or a license per dongle model, which allows the owner of the dongle use the software on any computer. A license may be perpetual (it lasts forever), or it may be for a fixed period (typically one year).

The software license often includes maintenance for a period (typically one year), and the maintenance agreement generally includes updates to the software during that time and it may also cover a limited amount of technical support. The two parties may sign a service level agreement (SLA), which stipulates the service that will be provided by the service provider. This will generally include timelines for the resolution of serious problems, as well as financial penalties that will be applicable where the customer service performance does not meet the levels defined in the SLA.

Free- and open-source licenses are often divided into two categories depending on the rights to be granted in distribution of the modified software. The first category aims to give users unlimited freedom to use, study, and modify the software, and if the user adheres to the terms of an open-source license such as the Free Software Foundation (FSF), GNU or General Public License (GPL), the freedom to distribute the software and any changes made to it. The second category of open-source licenses give the user permission to use, study, and modify the software, but not the right to distribute it freely under an open-source license (it could be distributed as part of a proprietary software license).

14.7 Testing and Prevention of Computer Crime

It is common in the major urban areas to encounter dangers in some streets or neighbourhoods, and such dangers need to be managed. Similarly, the Internet has dangers with hackers, scammers, and Web predators lurking in the shadows. A hacker may be accessing a computer resource without authorization with the intention of committing an unlawful act. The hacker's activities may be limited to *eavesdropping* (listening to a conversation), or it may be an active *man-in-the-middle* attack, where the hacker may possibly alter the conversation between two parties.

One of the earliest Internet attacks was back in 1988 when a graduate student from Carnegie Mellon University released a program on the Internet (an Internet Worm) that exploited security vulnerability in the mail software to automatically replicate itself locally and on remote machines. It affected lots of machines and effectively shut down the Internet for 1–2 days.

Today, more and more individuals and companies are on line, and networking systems and computers have become quite complex. There has been a major growth in attacks on businesses and individuals, and so it is essential to consider computer and network security. The Internet was developed based on trust with security features added as a response to different types of attacks.

There are several threats associated with network connectivity such as *unauthorized access* (a break-in by an unauthorized person), *disclosure of sensitive information* to people who should not have access to the information, and *denial of service* (DoS), where there is a degradation of service that makes it impossible to access the Web site and perform productive work.

There may be attacks that lead to defacement of the Web sites, bank fraud, theft of credit card numbers, hoax (scam) letters, and phishing emails that appear to come from legitimate parties but contain links to a site that is different from the one that the user expects to go to, intercepting of packets and password sniffing. *Phishing* is an attempt to obtain sensitive information such as usernames, passwords, and credit card details with the intention of committing fraud.

A computer *virus* is a self-replicating computer program that is installed on the user's computer without consent. It is a malicious software program that when executed replicates itself and infects other computer programs by modifying them. A virus often performs some type of harmful activity on the infected computers such as accessing private information, spamming email contacts, or corrupting data. It is not a crime per se to write a computer virus or malicious software. However, if that software or other malware spreads to other computers, then it could be considered a crime.

Cyberextortion is a crime that involves an attack, or threat of an attack, accompanied by a demand for money to stop the attack. They are often initiated through malware in an email attachment. These may include denial of service attacks or *ransomware* attacks that encrypts the victim's data. The victim is then offered the private key to resolve the encryption in return for payment. Companies need to manage the risks associated with cyberextortion and to ensure that end users are properly educated on malware and phishing.

Another form of computer crime is Internet fraud where one party is intent on deceiving another. Among these are hoax email scams, which are designed to deceive and fraud the email recipient. These may include the *Nigeria 419* scams, where the email recipient is offered a share of a large amount of money trapped in their country, if the recipient will help in getting the money out of the country. The recipient may be asked for their bank account details to help them to transfer the money (this information will later be used by them to steal funds), or the request may be to pay fees or taxes to release payment with further fees requested. Of course, the money will never arrive (*if an email looks like it really is too good to be true then it has a high probability of being a scam*).

Security testing of the software is important, as it is essential to identify any security vulnerabilities and to correct them. Further, it is important that users be educated to minimize risks of becoming victims of computer crime.

14.7.1 Testing and Hacking

A *hacker* is a person who uses his (or her) computer skills to gain unauthorized access to computer files or networks. A hacker may enjoy experimenting with computer technology (the original meaning of the term), but some hackers enjoy breaking into systems and causing damage (the modern meaning of the word). Ethical (*white hat*) hackers are former hackers who play an important role in the security industry in testing network security and in helping to create secure products and services. Malicious (*black hat*) hackers (also called *crackers*) are generally motivated by personal gain, and they exploit security and system vulnerabilities to steal, exploit or sell data (Fig. 14.3).

Many computer systems in use today have vulnerabilities that may be exploited by a determined hacker to gain unauthorized entry to the system and access to unauthorized information. It is vital that best practice in software and system engineering is employed to develop safe and secure systems, and that known vulnerabilities in system security are addressed promptly by updates to the system software. Further, it is essential to educate staff on security and to define (and follow) the appropriate procedures to prevent security breaches.

The early hackers were mainly young students without malicious intent who were exploring the university computer systems. These include the students at Massachusetts Institute of Technology in the late 1950s who were interested in exploring the IBM 704 computer, and they would enter areas of the system without authorization and gain access to privileged resources. They were motivated by knowledge and wished to have a deeper understanding of the systems that they had access to. The idea of a hacker ethic was formulated in a book by Steven Levy in the mid-1980s (Levy 1984), and he outlined several ethical principles including free access to computers and information and improvement to quality of life. His six key tenets are:

Fig. 14.3 Hacker at work on backlit keyboard. Creative Commons

- Access to computers should be unlimited and total
- All information should be free
- Mistrust authority
- Hackers should be judged by their hacking and not by bogus criteria such as race and religion
- Art and beauty can be created on a computer
- Computers can change your life for the better.

The *free software movement* arose in the early 1980s from followers of the hacker ethic, with Richard Stallman (its founder) often referred to as “the last true hacker” (O’Regan 2015). Today, ethical hackers need to obtain permission prior to acting, as their actions may potentially cause major disruption to an organization. Responsible (white hat) hackers can provide useful information on security vulnerabilities, and may assist by testing and improving computer security.

The security of the system refers to its ability to protect itself from accidental or deliberate external attacks, which are common today since most computers are networked and connected to the Internet. There are various security threats in any networked system including threats to the confidentiality and integrity of the system and its data, and threats to the availability of the system.

Therefore, controls are required to enhance security and to ensure that attacks are unsuccessful. Encryption is one way to reduce system vulnerability, as encrypted data is unreadable to the attacker. There may be controls that detect and repel attacks, and these controls are used to monitor the system and to take appropriate action to shut down parts of the system or restrict access in the event of an attack. There may be controls that limit exposure (e.g. insurance policies and automated backup strategies) that allow recovery from the problems introduced.

The introduction of the Internet in the early 1990s has transformed the world of computing, and it later led to an explosive growth in attacks on computers and systems, as hackers and malicious software sought to exploit known security vulnerabilities. It is therefore essential to develop secure systems that can deal with and recover from such external attacks.

Hackers will often attempt to steal confidential data and to disrupt the services being offered by a system. Security engineering is concerned with the development of systems that can prevent such malicious attacks, and recover from them. It has become an important part of software and system engineering, and software developers need to be aware of the threats facing a system and develop solutions to manage them.

Hackers may probe parts of the system for weaknesses, and system vulnerabilities may lead to attackers gaining unauthorized access to the system. There is a need to conduct a risk assessment of the security threats facing a system early in the software development process, and this will lead to several security requirements for the system.

The system needs to be designed for security, as it is difficult to add security after the system has been implemented. Security loopholes may be introduced in the development of the system, and so care needs to be taken to prevent these as well as preventing hackers from exploiting security vulnerabilities.

The choice of architecture and how the system is organized is fundamental to the security of the system, and different types of systems will require different technical solutions to provide an acceptable level of security to its users. The following guidelines for designing secure systems are described in Sommerville (2011):

- Security decisions should be based on the security policy
- A security-critical system should fail securely
- A secure system should be designed for recoverability
- A balance is needed between security and usability
- A single point of failure should be avoided
- A log of user actions should be maintained
- Redundancy and diversity should be employed
- Organization of information in system into compartments.

Security testing is carried out to identify any flaws in the security mechanisms of the computer system and to verify that the security requirements such as confidentiality, availability, integrity, etc., are satisfied. However, the successful completion of security testing does not guarantee that there are no security vulnerabilities in the system.

The unauthorized access to a computer system and the theft of confidential data and disruption of its services is unlawful and may be subject to prosecution and the full rigour of the law.

14.8 Review Questions

1. What is intellectual property law?
2. Describe the behaviours of the ethical software tester
3. How can a software company demonstrate that it took all reasonable steps to deliver a high-quality software product, and that the testing was fit for purpose
4. Explain the different types of software licensing
5. Explain the legal aspects of bespoke software development
6. What happens when one party in a test-outsourcing project believes that a material breach of the contract has occurred?

7. What types of lawsuits could be brought against a software company?
8. Explain the difference between ethical and malicious hackers
9. What is computer crime?
10. Explain cyber extortion.

14.9 Summary

Legal aspects of testing are concerned with the application of the legal system to the computing field. It includes intellectual property law including patents, copyright, trademarks and trade secrets; bespoke software development; test outsourcing; licensing of software; professional negligence in the development and testing of software; and computer crime.

A lawsuit is a proceeding by a party against another party in a civil court where the plaintiff sues another person for being negligent, and the negligence of the defendant caused injury or damage to the property of the plaintiff.

Bespoke software (or custom software) is software that is developed for a specific customer or organization and needs to satisfy specific customer requirements. The legal contract specifies the obligations of the supplier, and should the supplier fail to honour its commitments it may well be in breach of contract. This may result in the first party seeking a legal remedy in a civil court.

A software license is a legal agreement between the copyright owner and the licensee, which governs the use or distribution of software to the user (licensee). Computer software code is protected under copyright law, and the license grants the user permission to make one or more copies of the software. Software license agreements generally provide limited remedies to the customer when the software defective. However, there may be legal implications if the software has been inadequately developed and tested.

A hacker is a person who uses his (or her) computer skills to gain unauthorized access to computer files or networks. Hackers may probe parts of the system for weaknesses, and system vulnerabilities may lead to attackers gaining unauthorized access to the system. The system needs to be designed for security, as it is difficult to add security after the system has been implemented. Security loopholes may be introduced in the development of the system, and so care needs to be taken to prevent these as well as preventing hackers from exploiting security vulnerabilities.

References

Barquin RC (1992) In pursuit of a ‘ten commandments’ for computer ethics. Computer Ethics Institute, Washington, D.C.

Levy S (1984) Hackers: heroes of the computer revolution. O’Reilly Media, Sebastopol

O’Regan G (2015) Pillars of computing. Springer, Berlin

Sommerville I (2011) Software engineering, 9th edn. Pearson, London