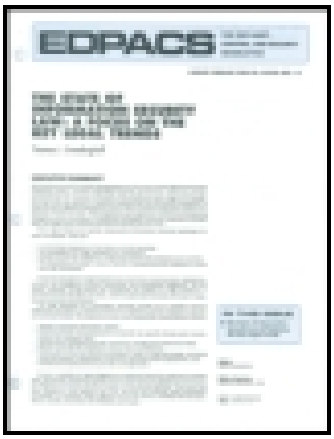

EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

The Role of Legislation in Information Security

Corey Schou PhD [a]

[a] Idaho State University , Pocatello, USA

Published online: 05 Jan 2010.

To cite this article: Corey Schou PhD (1993) The Role of Legislation in Information Security, EDPACS: The EDP Audit, Control, and Security Newsletter, 20:10, 1-8, DOI: 10.1080/07366989309451622

To link to this article: http://dx.doi.org/10.1080/07366989309451622

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

APRIL 1993 VOL. XX, NO. 10

THE ROLE OF LEGISLATION IN INFORMATION SECURITY

COREY SCHOU

This article and one that will appear next month will provide the information systems auditor and information systems security specialist with a basic framework for understanding the role of law in planning, implementing, and sustaining a truly comprehensive information security program.[1]

These articles focus primarily on US legislation and court cases. They do not purport to provide specific legal advice about any particular situation. A pair of articles on this topic cannot hope to address all areas of the law that might be relevant to information systems security. Local variations of general principles and the application of the law relating to the possession and control of real property; the torts of false arrests, malicious prosecution, libel, slander, conspiracy to injure, interference with advantageous business relationships, and conversion; and numerous other aspects of this topic are not dealt with in detail in these articles.

There are several underlying areas of common interest for the information systems security specialist and the information systems auditor. Policies and procedures must be established that control the use of information systems hardware and software as well as protecting the organization from fraud, the physical abuse of these assets, the misuse of data or information, and invasions of personal privacy.

THE CONTROL OF INFORMATION SYSTEMS HARDWARE

When computers first began to be used widely some 30 years ago, a few enterprising individuals also saw the potential of these machines for their personal gain. These people began to match their wits against these machines and to find ways to use the computer for criminal purposes. The average armed robbery nets about $9,000 and the average computer fraud totals about $450,000. This is a high-yield, low-risk crime.

One area of computer crime is the theft of information systems hardware and software. The outright theft of hardware and software often is reported and identified as the prime

IN THIS ISSUE

AUERBACH PUBLICATIONS
Warren Gorham Lamont
A Division of Research
Institute of America

motive for a crime. In one incident, more than $300,000 worth of computer equipment was stolen using fictitious invoices. Sometimes only parts of the computer are targeted. Several of Digital Equipment Corp. installations have experienced break-ins resulting in the theft of VAX printed microcircuit boards. One theft consisted of 22 boards worth about $450,000.

THE AVERAGE ARMED ROBBERY NETS ABOUT $9,000; THE AVERAGE COMPUTER FRAUD TOTALS ABOUT $450,000.

The computer creates a unique environment in which unauthorized activities can occur. Crimes in this category have many traditional names, including theft, fraud, embezzlement, and extortion. Computer-related fraud includes the introduction of fraudulent records into a computer system, the theft of money by electronic means, the theft of financial instruments, the theft of services, and the theft of valuable data.

Physical abuse of information systems hardware frequently is overlooked as an issue in the design of the information system. The computer can be the object of the attack in computer crimes.

Some examples include the unauthorized alteration or destruction of information, data file sabotage, and vandalism against a computer system. Computers have been shot, stabbed, short-circuited, and bombed.

Information is an asset of an organization; it must be protected carefully. Computers and their associated information systems can be used symbolically to intimidate, deceive, or defraud victims. Attorneys, government agencies, and business organizations increasingly use mounds of computer-generated data quite legally to confound their audiences. Criminals also find fictitious invoices, bills, and checks generated by a computer useful in their schemes. The computer lends an ideal cloak for carrying out criminal acts by imparting a clean quality to the crime.

The computer has made the invasion of personal privacy a great deal easier and potentially more dangerous than was true before it arrived. A wide range of data related to individuals is collected and stored in computerized files. These include information on banking transactions, credit experience, organizational fund-raising activities, response to opinion polls, use of shop-at-home services, the issuance of driver's licenses, arrests, and medical services. The potential threats to privacy include the improper commercial use of computerized data; breaches of confidentiality that can occur when sensitive, private, and personal data is made available to third parties; and the release of records to governmental agency investigations.

If you have information of interest to EDPACS, contact Eric Birenbaum, Senior Editor, Auerbach Publications, Warren Gorham Lamont, a division of Research Institute of America Inc., One Penn Plaza, New York NY 10119. EDPACS (ISSN 0736-6981) is published monthly by Auerbach Publications, Warren Gorham Lamont, a division of Research Institute of America Inc., 210 South St., Boston MA 02111-2797, (617) 423-2020. The subscription rate is $142/year in the US. Prices elsewhere vary. Printed in USA. Second class postage is paid at Boston MA. Postmaster: Send address change to EDPACS, Auerbach Publications, 210 South St., Boston MA 02111-2797.

The EDP Auditors Association Inc (EDPAA) is the only professional association dedicated to information systems auditing. Founded in 1969, the EDPAA represents information systems audit professionals in 52 countries. The EDPAA fosters professionalism through information transfer, certification, communication, and education. For more information, contact: The EDPaa, PO Box 88180, Carol Stream IL 60188.

Personal data privacy must be maintained by the organization at all times in order to comply with applicable US laws. The Fourth Amendment to the US Constitution specifies that people have a right to be secure in their homes and against unreasonable searches and seizures. Many additional laws have been enacted to protect the individual from the unauthorized disclosure of damaging personal information and from having such information stored in computerized data bases.

LAWS AND LEGISLATION

For some time, prosecutors in the US and elsewhere have faced some uncertainty when they have attempted to use existing criminal statutes to prosecute computer-related offenses. Within recent years, this situation has improved in the US at least with the addition of computer crime statutes to the US Code and to the statutes of many states.

Computer crime laws encompass the act of trespassing into a computerized system; the invasion of the privacy of an individual; the theft of money, service, data, or programs from a computerized system; and the alteration or destruction of data. The laws also can be used to prevent or deter computer-related fraud and the misuse of computerized information.

The law provides compensation for injuries and deters wrongdoers through the smooth and efficient operation of the legal system. The law, generally, does not provide a remedy if no injury has occurred. Thus, the law acts as a shield through its deterrent effect and not in a proactive manner. On the other hand, after a wrongdoer has compromised physical or environmental security arrangements, the law is the only tool available to the information security specialist for minimizing the injury already done and for deterring, as far as is possible, future wrongdoing.

One way of maintaining computer security is by a knowledge of the appropriate laws and legislation. These laws become important tools in forming policy and regulations. The laws dealing with privacy are currently changing. The loss of privacy is a danger associated with the proliferation of computerized data banks. The computer's ability to collect, store, and manipulate vast amounts of data and its ability to retrieve selected items from these data banks almost instantaneously allows the collection and distribution of personal information that can compromise people's privacy. One of the primary defenses against the loss of individual privacy is the enactment of legislation by national and state legislatures. The basic concern of this privacy legislation has been the control and protection of information on or about individuals.

Privacy protection laws have been passed in most developed countries. Early in 1970, the US introduced the Fair Credit and Reporting Act, which governs the processing of, access to, and the disclosure of information about an individual's credit history and status. The US Privacy Act of 1974, as amended (Title 5, USC § 552a), and the Canadian Privacy Act of 1975 are examples of laws that mandate the protection of individual privacy. Other countries also have enacted laws related to individual

THE COMPUTER HAS MADE THE INVASION OF PERSONAL PRIVACY A GREAT DEAL EASIER AND POTENTIALLY MORE DANGEROUS THAN WAS TRUE BEFORE IT ARRIVED.

privacy. These include the Swedish Data Act of 1973, the German Federal Data Protection Act of 1977, the French Act On Data Processing of 1978, the Danish Acts on Private Registers, and the Austrian Federal Data Protection Act of 1978. At the international level, the OECD Transborder Data Flow Guidelines address the movement of information across international borders, perhaps to jurisdictions in which privacy laws may differ from those of the country in which the information in question originated.

ONE WAY OF MAINTAINING COMPUTER SECURITY IS THROUGH KNOWLEDGE OF THE APPROPRIATE LAWS AND LEGISLATION.

INTELLECTUAL PROPERTY

Another way of protecting the organization is by using the intellectual property laws. These statutes relate to secrets, names, ideas, and other similar concepts. The creator of this type of property has certain rights to it. This is true whether the property is a book, a play, a computer program, or a musical composition. Four bodies of intellectual property laws protect different aspects of this property and their use.

Patent Law

A patent can protect the unique and secret aspect of an idea. It is very difficult to obtain a computer software patent compared to a copyright. When a piece of computer software is at issue, complete disclosure of it is required. The patent holder must disclose the particulars of the program in sufficient detail to allow another person who is skilled in the process of programming to build the program. A US software patent will be unenforceable in most other countries.

Trade Secrets Law

A trade secret is something held in confidence that possesses a definable value and usefulness. This law protects the unique and secret aspects of ideas, known only to the discoverer or that person's chosen confidants. Once disclosed, the trade secret is lost as such and can be protected only under one of the other intellectual property laws. This is very important in the computer field, where even a slight head start in the development of either software or hardware can provide a significant competitive advantage.

Trademark Law

Protecting the name given to a software product often is as important as protecting the software itself. Trade names for well-known products have gained great value as their commercial recognition has increased. Trademark laws exist under both state common laws and US statutes. Trademark rights arise on the first use of the trademark in commerce. Trademarks should be used to protect the names of any software packages that an organization may develop. Simply using a trademark to identify an entity gives one common law rights to continue using this designation. If the trademark is regis-

tered with the US Patent and Trademark Office, the holder acquires the rights to use the trademark anywhere that business is being conducted.

Copyright Law

Copyright law provides a significant legal tool for protecting computer software, both before a security breach occurs and certainly after such a security breach takes place. This type of violation could involve the misappropriation of data, computer programs, documentation, or similar material. For this reason, the information security specialist will want to be familiar with basic concepts related to copyright law.

IT IS VERY DIFFICULT TO OBTAIN A COMPUTER SOFTWARE PATENT COMPARED WITH A COPYRIGHT.

The act of declaring the existence of a copyright gains the protection of the copyright laws for the intellectual property involved. The proper form is simple and involves the display of the word *copyright* or the symbol ©, the year of first use, and the name of the entity declaring the copyright. The use of the symbol © gains copyright protection in certain countries outside the US. One may choose to add the words *all rights reserved* to this declaration. This statement limits the ability of others to reproduce the work in question without the express written permission of the entity declaring the copyright. In the US, one may file copies of the copyrighted item with the Copyright Office in the Library of Congress to formalize the assertion of the copyright.

The US, the United Kingdom, Australia, and many other countries now have amended or revised their copyright legislation to provide explicitly that computer programs are protected by copyright law. Copyright law in the US is governed by the Copyright Act of 1976, which preempted the field from the states. (Formerly, the US had a dual state and federal government copyright system.) In other countries, such as Canada, the courts have held that the unrevised Copyright Act is broad enough to protect computer programs. In many of these countries, the reform of copyright law is under way actively. The format of the protected intellectual property is quite varied. Although one usually thinks of copyrightable software as having the form of listings on disks or printouts, a US federal district court ruling also has protected microcode placed on chips. In the Intel dispute with NEC, it was ruled that copyrights can cover semiconductor microcode.[2]

Federal laws, such as the Privacy Act of 1974 and the Foreign Corrupt Practices Act, were used to combat computer crime during the late 1970s and early 1980s. The Computer Crime Bill of 1978, sponsored by then US Senator Abraham Ribicoff (Democrat—Connecticut), was used as the basis for many of the initial state computer crime laws as well as for subsequent federal legislation. During 1984, congress, within several bills, enacted the first US statutory provisions specifically outlawing certain types of computer abuse. These provisions prohibited the unauthorized use of computers in three areas:

- ☐ They made it a felony to access a computer to obtain classified military or foreign policy information.

- ☐ They prohibited access to a computer to obtain financial or credit information without authorization.
- ☐ They made it a misdemeanor to access a US government computer to modify or destroy data.

COMPUTER SECURITY ACTS

US STATES HAVE TAKEN THE LEAD IN ESTABLISHING COMPUTER SECURITY LAWS.

The Federal Computer Crime Act was put in place in 1984. It provided criminal penalties only for stealing national security–related data or for trespassing into the government's computers and computerized information about the credit histories of individuals. During 1986, the 99th US Congress modified Title 18 of the US Code, which includes Section 1030 (fraud and related activity in connection with computers). These made it clear that acts of simple trespass into government computers are punishable, authorized prosecution of those who traffic in computer passwords, and strengthened the Federal Computer Crime Act by expanding the range of the data protected beyond purely US government agency data bases to the government-related data held by other entities, such as banks and financial institutions.

The Computer Security Act of 1987 provided for maintaining a computer standards program within what is now known as the US National Institute for Standards and Technology (NIST). This act stated that NIST would:

- ☐ Be responsible for developing standards and guidelines related to security and privacy for federal government computer systems.
- ☐ Provide mandatory periodic training in computer security to all employees involved with the management, the use, or the operation of federal government computer systems.

The act also provided that the US Department of Defense and its National Security Agency would continue to be responsible for the security of the government's classified computer systems.

STATE LAWS

In many cases, individual US states have taken the lead in establishing computer security laws. The first 10 states to adopt computer crime legislation were Arizona, California, Colorado, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, and Utah. Thirty-eight additional states also have passed computer crime legislation. These laws usually define various aspects of computer crime in great detail—including such terms as "the theft of services," "the criminal use of a computer," "deceiving a machine," "computer fraud," "computer program," and "computer network." The approaches to these issues and the provisions of these laws vary by state. Many also specify maximum fines and punishments:

- ☐ California's computer crime law specifies a maximum $10,000 fine for accessing a computer for the purposes of extortion.
- ☐ The Louisiana law specifies that, on conviction, an offender may be fined not more than $10,000 and imprisoned for not more than five years.

- ☐ In Maryland, the sanctions for violations are limited to fines of $1,000 or less, and imprisonment is not to exceed three years.
- ☐ In the Minnesota law, damage or destruction of hardware is designated as an offense. Maximum fines are specified at not more than $10,000.
- ☐ The Montana law mentions such things as the value of the electronic impulses, electronically produced data, and computer software. The statute attempts to define the value of these.
- ☐ In the Nevada law, denial of the use of a computer is defined as an "unlawful act."
- ☐ The New Jersey law defines alteration and destruction of data as a crime.
- ☐ The North Carolina law mentions the use of a computer in extortion.
- ☐ The Oklahoma law specifies a maximum fine of $100,000.
- ☐ The Washington law uses the term "computer trespass" rather than "access."
- ☐ The Wyoming law addresses the theft of trade secrets and intellectual property.
- ☐ The Connecticut law has provisions that protect the privacy of individuals, including the elimination of governmental immunity.

Additional state computer crime–related statutes are being added each year. For example, 13 state legislatures proposed some 21 pieces of computer crime legislation during their 1987 sessions. During their 1988 sessions, seven additional states considered legislation in this area. These bills proposed new definitions of computer crime, revised definitions of the terms used in existing laws, enhanced penalties, authorization for certain agencies to conduct computer crime investigations, and compensation procedures for victims of computer crimes.

A proposed California statute would broaden greatly the state's authority to prosecute computer crimes. The bill has been criticized as too harsh. As proposed, the statute provides that:

- ☐ Punishment for unauthorized access to a computer would be determined not only on the dollar value of the computer time used but also by the expense of assessing and repairing the damage done to the system.
- ☐ The plaintiffs burden of proving the malicious intent by the defendant would be eliminated in this instance.
- ☐ The seizure and confiscation of items taken as the result of a warrant or arrest would be permitted. Such items could be destroyed or distributed to a public entity or nonprofit corporation.

A bill considered by the Illinois Senate legislature provided for forfeiture of any monies, profits, or proceeds acquired directly or indirectly as the result of a computer crime. Many of these bills refine or enhance existing laws:

- ☐ An Idaho senate bill defined computer crime within the definitions of trade secrets.
- ☐ The Massachusetts state legislature is considering a bill that establishes a commission to determine and review the adequacy of current laws defining computer crime.

INFORMATION IS AN ASSET OF AN ORGANIZATION THAT MUST BE PROTECTED CAREFULLY.

- ☐ Both the New Mexico and North Dakota state legislatures have passed legislation that further defines or redefines computer crime and computer fraud.
- ☐ The Utah state legislature has passed legislation to provide for compensating the victims of computer crime.
- ☐ The Texas legislature has passed legislation related to the intellectual property policies of the state's institutions of higher education. One of the matters addressed in these bills was the disclosure of scientific and technological developments, including computer software. This act provides a basis for the control and protection of computer software developed at institutions of higher education in Texas.

THE UTAH STATE LEGISLATURE HAS PASSED LEGISLATION TO PROVIDE FOR COMPENSATING THE VICTIMS OF COMPUTER CRIME.

MODEL COMPUTER CRIME BILL

It is apparent from reading many of these laws and bills that, in the US, at the state level, legislation that attempts to deal with various aspects of computer crime is neither uniform nor consistent. In one reaction to this situation, the Data Processing Management Association (DPMA) has drafted the Model Computer Crime Act. This act:

- ☐ Defines computer crime.
- ☐ Establishes civil procedures for the redress of victims of computer crime.
- ☐ Offers guidelines (essentially an amendment of the rules of evidence) for what evidence will be considered in a computer crime case.
- ☐ Suggests punishments, including forfeiture of property and increased penalties for repeated violations, and addresses the issue of jurisdiction.

Jurisdiction is a significant problem for the courts because the computer criminal may reside in one state or country while committing a crime in another via data communications systems.

Information systems auditors and information security specialists should attempt to keep abreast of continuing developments in computer crime–related legislation. Strengthening existing laws in this area only can have a positive impact on the problems being addressed. And they may deter a few would-be perpetrators of computer crime. ■

Corey Schou, PhD, is associate professor of computer information systems and chair of computer information systems, Idaho State University, Pocatello. He has developed management information and training systems for such organizations as the Florida State Parole Commission, Industrial Boiler, and General Motors Corp. Schou compiled and edited the computer security education course materials for the US government.

Notes

1. A summary of 13 relevant US cases related to the issues discussed in these two articles will appear in next month's issue.
2. As reported in *PC Week* in April 1989.