CSIT115 Data Management and Security

Legal and Ethical Issues in Data Management

Dr Janusz R. Getta

School of Computing and Information Technology -
University of Wollongong

Legal and Ethical Issues in Data Management

Outline

Legal and Ethical Dilemmas

Legal and ethical dilemmas of database administrators are caused by:

- unrestricted access to confidential and valuable information in read and write mode
- unrestricted access to historical information in read and write mode

Why do we have to worry about ethics in data management ?

- Conduct and character of people involved in data management
- Professional and unprofessional behaviour of people involved in data management
- Increasing pressure from organized/unorganized crime organizations on access to valuable data
- Growing amount of sensitive data stored electronically
- Wide access to sensitive data

Ethics is a set of principles of correct conduct or a theory or a system of moral values (one of many possible definitions)

Ethics versus Legislation

What is ethical - is legal ?

What is unethical - is illegal ?

Is all unethical behaviour illegal ? (No, not all behaviour is legalized)

Is all ethical behaviour legal ? (No, there exist legal loopholes)

Examples of unethical behaviour in IT

- Installation of unlicensed software, accessing personal information, divulging trade secrets, etc (~57% of IT personnel has been asked to do so)
- Read and write access to the outcomes of data mining and data warehousing historical analysis

IT Governance: Activity used for specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT

Legal and Ethical Issues in Data Management

Outline

Legislation

Securities and Exchange Commission's (SEC) regulation National Market System(NMS)

- Order protection rule: purchasing large block of shares at an inferior price
- Financial services firms are required to collect and store market data such that it is possible to demonstrate that better price was not available at the time trade was executed

The Sarbanes-Oxley act, COBIT and COSO

- Companies must certify accuracy of their financial data => increased requirements of security and auditing of financial data =>it has implications on how data is collected, processed, and secured
- Companies must adopt a formal control framework for information management risks:
- Control Objectives for Information and related Technology (COBIT 5 2012)
- Committee of Sponsoring Organizations of the Treadway Commission(COSO 1996)

Legislation

COBIT 5 Processes

- Governance of Enterprise IT: Evaluate, Direct, and Monitor (EDM) ensures governance framework setting and maintenance, benefits delivery, risk optimization, resource optimization, and stakeholder transparency
- Management of Enterprise IT: Align, Plan, and Organize (APO) covers use of information an technology and how the best it can be used in an organization to achieve the organization's goals and objectives; highlight the organizational and infrastructural form IT suppose to take to achieve the optimal results and maximum benefits
- Management of Enterprise IT: Build, Acquire, and Implement (BAI) identifies IT requirements , acquiring the technology, and implementing current business processes
- Management of Enterprise IT: Deliver, Service, and Support (DSS) covers execution of the applications within the IT system, and tis results, support of processes that enable effective efficient data processing within IT systems

Legislation

COBIT 5 Processes

- Management of Enterprise IT: Monitor, Evaluate, and Assess (MEA) assesses organizations's strategies, verifies whether IT system meets the objectives, controls consistency with the regulatory requirements; assesses effectiveness of IT system to meet business objectives and organization control processes by internal and external auditors

Legislation

The Health Insurance Portability and Accountability Act

- Privacy of patient information: patients are required to sign consent form to allow their healthcare providers to share medical information with other providers and insurers
- Standarizing electronic health/medical records and transactions between healthcare organizations: a number of standards have been developed to cover typical healthcare transactions such as claims, enrolment, patient eligibility, payments, etc.
- Establishing a nationally recognized identifier for employees to be used by all health plans: such identifier is used in all subsequent transactions between healthcare organizations
- Standards for the security of patient data and transactions involving this data: patient data must be secured both within database systems as well as when transmitted between the organizations
- Need for a nationally recognized identifier for healthcare organizations and individual providers: similar to those for the standarized employee identifier

Legislation

The European Union Directive on Data Protection

Principles:

- Subjects whose data is being collected should be given notice of such collection
- Data collected should be used only for stated purposes and for no other purposes
- Personal data should not be disclosed or shared with third parties without consent from its subject
- Once collected, personal data should be kept safe and secure from potential abuse, theft, or loss
- Subjects whose personal data is being collected should be informed about disclosure as to the party or parties collecting such data
- Subjects should be granted access to their personal data and to correct any inaccuracies
- Subjects should be able to hold personal data collectors accountable for adhering to all of these principles

In 2012 The European Commission unveiled a draft legislative package to create a single European data protection law

Legislation

Draft legislative package to create a single European Data protection Law (2012)

Proposed changes include:

- Applicability of the law for all non-EU companies without any establishment in EU
- Any processing of personal data will require clear information to be provided to concerned individuals as well as specific and explicit consent to be obtained from such individuals for the processing of their data
- Making a safe transfer of data outside of the EU (including data in clouds) easier in the event that the parties involved commit themselves to binding corporate rules
- New privacy rights including data subject's right of portability and right to be forgotten will be established
- The processing of data of individuals under the age 13 will normally require parental consent
- Companies must notify EU data protection authorities as well as the individual whose data are concerned by any breaches of data protection regulations or data leaks within 24 hours from discovering the breach

Legislation

Draft legislative package to create a single European Data protection Law (2012)

Proposed changes include:

- Harsh sanctions where breaches of the unified EU data protection laws occur, with penalties up to 2% of a company worldwide turnover for severe data protection breaches

Legislation

The United Kingdom's Data protection Act of 1998

Principles:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless it is consented or necessary
- Personal data shall be obtained only for one or more specified lawful purpose, and shall not be further processed in any matter incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed
- personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the right of data subjects under this Act
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Legislation

The United Kingdom's Data protection Act of 1998

Principles:

- Personal data shall not be transferred to a country outside European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Legislation

International Banking - Basel II Accords (2004)

Principles:

- Minimum capital requirements: institutions must maintain sufficient funds given the level of risk inherent in their portfolio of assets; the measurements of risk include:credit risk, market risk, interest rate risk, and operational risk
- Supervisory review process: management must understand and actively control the risks, have sufficient internal risk controls,and timely reporting,including compensation plans that reward appropriate risk management behavior
- Market discipline: institutions must publicly disclose information about their capital adequacy, risk exposure, and the processes by which they measure and mitigate risks

Legal and Ethical Issues in Data Management

Outline

Legal and Ethical Data Stewardship

Organization-wide policy for legal and ethical behavior:

- Awareness of legislation in industry practice
- Data administrators and CIOs asses how legislation affects the flow of data within the organization
- New or revised operating procedures must be documented and communicated to all affected parties
- Once legal parameters conducting business have been developed a similar set of ethical principles should be developed
- Lapse in legal an ethical behavior must be dealt swiftly and fairly within guidelines known to all employees

Legal and Ethical Data Stewardship

Professional organizations and code of ethics

- The ACM Code of Ethics and Professional Conduct (ACM, 1992); Four main categories: fundamental ethical considerations, specific considerations of professional conduct, considerations for individuals in leadership roles, compliance with the code
- The 2011 British Computer Society Code of Conduct; Four main areas: public interest, professional competence and integrity, duty to relevant authority, duty to the profession

Legal and Ethical Issues in Data Management

Outline

Intellectual Property

Intellectual property is the product of human creativity in the industrial, scientific, literary, and artistic fields

Intellectual property includes inventions, inventive ideas, designs and design rights, written work(including computer software), know-how devised, developed, or written by an individual or set of individuals

We distinguish two types of IP:

- Background IP that exists before an activity takes place
- Foreground IP that is generated during an activity

There are three ways to protect IP rights:

- Patents
- Copyright
- Trademark

Intellectual Property

Patent provides an exclusive (legal) right for a set of period of time to make, use, sell, or import an invention

Patents are granted by a government when an individual or organization can demonstrate that invention is new, useful, and it involves inventing step

Patent must disclose how the invention works

Patents give effective protection for new technology that will lead to a product, composition, or process with significant long-term commercial gain

Artistic creations, mathematical models, plan, schemes, or other purely mental process cannot be patented

Intellectual Property

Copyright provides an exclusive (legal) right for a set of period of time to reproduce and distribute a literary, musical, audiovisual, or other "work" of authorship

Copyrights are granted through a formal application process and it comes into effect as soon as what is "created" takes a fixed form

Copyright cover books, articles, song lyrics, music, videos, TV programs, public lectures, computer software, databases, technical drawings, designs, and multimedia

Copyright holders can sell the rights to their works to individuals or organizations in return for payments also called as "royalties"

Copyright also gives moral rights to be identified as the creator of certain kind of material and to object to distortion or mutilation of it

Intellectual Property

Trademark provides an exclusive (legal) right use a word, symbol, image, sound, or some other distinctive element that identifies the source of origin

Trademarks are intended to be associated with specific goods and services and as a result they assist consumers in identifying the nature and quality of the products they purchase

Trademark gives the owner exclusive legal rights to use, license, or sell the goods and services for which it registered

Intellectual Property

Copyrights apply to all software and the distribution and use of software is subject to license that determines the terms of use

There are four types of license:

- Commercial software perpetual use: fee is paid for the software and the license allows the software to be used for as long as you like and to make copies only for the purpose of backup if something goes wrong with the machine
- Commercial software annual fee: fee is required for each year of continued use and in most cases the software stops working unless the fee is paid and a new license key is issued by the supplier
- Shareware: software is available for free "trial"period
- Freeware: software is available free for certain categories of use; there are two categories of freeware: software distributed without source code and open source software; a license determines the terms and conditions of free use, e.g. software cannot be used for commercial purposes

References

T. Connoly, C. Begg, Database Systems, A Practical Approach to Design, Implementation, and Management, Chapter 21 Professional, Legal, and Ethical Issues in Data Management, Pearson Education Ltd, 2015