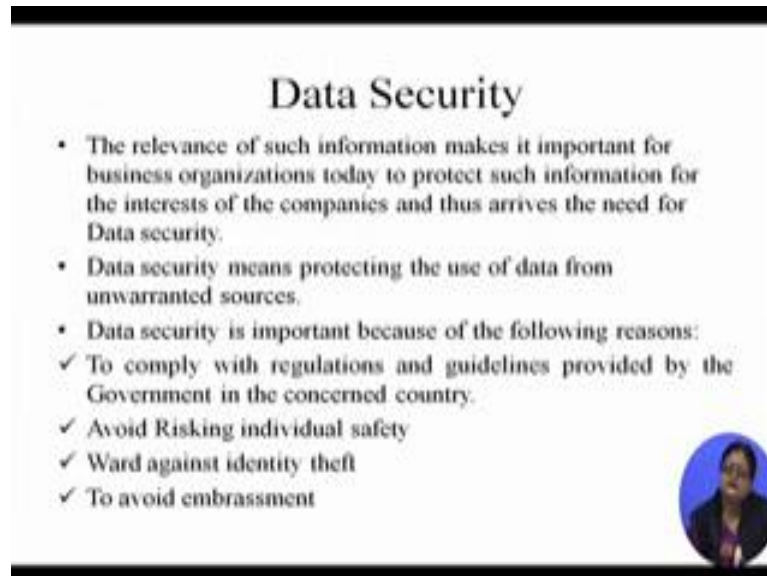


Business Ethics
Prof. Susmita Mukhopadhyay
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Lecture – 59
Data identity and security

(Refer Slide Time: 00:28)



Data Security

- The relevance of such information makes it important for business organizations today to protect such information for the interests of the companies and thus arrives the need for Data security.
- Data security means protecting the use of data from unwarranted sources.
- Data security is important because of the following reasons:
 - ✓ To comply with regulations and guidelines provided by the Government in the concerned country.
 - ✓ Avoid Risking individual safety
 - ✓ Ward against identity theft
 - ✓ To avoid embarrassment

So, in the last module we discussed about data security and why data security is important, the reasons why it is important. Now we will be discussing, the risk management issues with respect to data security. So, to secure risk management business corporations have to take certain steps in creating a new corporate culture, that is conscious of information security. So, the features that may help in risk management with respect to data are first is awareness.

Information security awareness programs within the corporations are the beginning steps of developing a corporate culture for information security. The human resource department should take proper responsibility to initially acquaint the employees with the importance of information security. Cross functional themes are risk councils, then securities steering committee and the other committees like these have to act together to in their information security objective.

So, with these coordinated effort it requires like, it reduces the duplication cost. Third which is very important is the management commitment. The culture of an organization

usually depicts the reasoning behind in the activities taken and the goals. So, when it is the culture of the organization to be assertive on information security then, it filters down from the top employee to the last employee. So, what is the approach taken by the organization in the assessment of the actual risk and their constant review helps the people to understand the real risk and rather than follow some systems blindly.

So, an intentional approach to security can help to select appropriate control and to mitigate the risk. So, and a balance has to be done between the risk management support, competent people, the needs of the employees, the employees privacy, the technology, then techniques taken for monitoring. So, these type, it has to be a balance between all these factors. So, if the initiative is taken by the business organization for risk management with respect to information security. So, it puts the business on a very good like business module, but it also have a trustworthy module to follow.

So, how this can be done? If this culture has to be achieved of awareness, cross functional team, the commitment managerial, management commitment and then approach then this gets its reflection that through the processes developed in the organization. So, what are the IT processes? So, what are the responsibility of the organization to themselves and to its different stakeholders other concerns when we are talking of the IT processes and the three things which becomes important over here are; prudence, due care and due diligence.

Whenever we are talking of prudence, it is the, we know like it is the judgment of the people who are responsible for running the system. So, how to increase the security? How to inbuilt safety measures? So and how to manage the affairs of information so that it is not misused by some unauthorized people and loosing this information to unwanted and unauthorized people. Due care should be taken to protect the interest of the stake holders, so that they can entrust their most treasured information, and reputation in the hands of the able managers.

And for this, this is actually a principle agency relationship and to exercise this due care the honesty of the person, the integrity of the person, agent who is interested with this responsibility to cross check to see there is no major conflict of interest happening with this person are important for this due care to be taken for the most treasured information of the stakeholders, who have entrusted you with the responsibility of the proper use of

those information. And the third virtue which is most important over here is the, due diligence is; due diligence is the foremost virtue in the eyes of law.

Today due diligence in the matter of information security plays a big role in area such as in the capital market. So, when you talking of due diligence, it is the disclosures and declarations are true to the information that the company possesses and falsifying of data can lead to various problems, seen in a broad spectrum, so IT is a common good for the benefit of all. So, for the IT professionals have a special responsibility to be the, like in a towards of this technology and then they the service demands like a competent people delivers these services and they respect other people's privacy and property are protected.

So, information security processes are also backed by laws to govern the use of information security. So, all countries mostly have enacted laws to ensure the integrity of the data, the privacy of the people who have shared their data and so and to prevent from its possible misuse and to prevent from the possible misuse of the data and the protection of the businesses.

(Refer Slide Time: 11:25)

Laws related to Data Security			
The table below provides the list of laws framed for Data security.			
Area	Act	Date	Description
Telecommunications	Telecommunications Regulation and Competition Act of 1996... Update to Communications Act of 1934 (47 USC 151 et seq.)	1996	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (HQA)	1966	Allows for the disclosure of previously withheld information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976--Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unauthorized Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications such as e-mail and documents stored by a service provider
Frauds to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computing (18 USC 1030)	1986	Defines and formulates laws to deter threats from computer-related activities (amended 1996, 2001, 2008)

So, let us now see some of these laws which are there with relevance to data security. So, what we find may be over here the, if you goes back to the date it is from way back in 1934, that you find like, laws are there for like telecommunication, freedom of information; which is 1966 and privacy, copy right; 1976, which deals with the

protection of the intellectual property including publication and software. We will be discussing intellectual property in details in the next modules. So, cryptography, where which deals with the, regulates interception and disclosure of electronic information, then access to stored communication, then provides penalties for illegally axing stored communication such as email and voice mail stored by a service provider. Threats to computers for computer fraud and abuse act which is then again 1986.

(Refer Slide Time: 13:14)

Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Trap and trace restrictions	General prohibition on pen register and trap and trace device use; exception (18 USC 3121 et seq.)	1993	Prohibits the use of electronic "pen registers" and trap and trace devices without a court order
Criminal intent	National Information Infrastructure Protection Act of 1996 (amends to 18 USC 1030)	1996	Categorizes crime based on defendant's difficulty to access a protected computer system and criminal intent
Trade secrets	Economic Espionage Act of 1996	1996	Prevents abuse of information gained while employed elsewhere
Personal health information protection	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information
Encryption and digital signatures	Security and Freedom Through Encryption Act of 1997	1997	Affirms the rights of persons in the United States to use and sell products that include encryption and to relax export controls on such products
Intellectual property	No Electronic Theft Act Amends 17 USC 1066a--copyright infringement, and 18 USC 2319--criminal infringement of copyright (Public Law 105-147)	1997	Amends copyright and criminal statutes to provide greater copyright protection; penalties for electronic copyright infringement

So, formalizes laws to counter threats from computer related acts and offences. Federal agency information security, then you find criminal intent, categories crimes based in deferments, authority to access of protected computer system and criminal intent will be discussing. The different types of crimes and punishment in the next modules like, economic espionage act regarding trade secrets, personal health protection, digital encryption and digital signatures, intellectual property.

(Refer Slide Time: 13:57)

Area	Act	State	Description
Copy protection	Digital Millennium Copyright Act (update to IT USC 1011)	1998	Provides specific penalties for removing copyright protection from media
Identity theft	Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028)	1998	Attempts to investigate specific penalties for identity theft by identifying the individual who loses their identity as the true victim, not just those commercial and financial credit entities who suffered losses
Banking	Gramm-Leach-Bliley Act of 1999 (GLBA) or the Financial Services Modernization Act	1999	Repeals the restrictions on banks relating with insurance and securities firms, has significant impact on the privacy of personal information used by these industries
Terrorism	USA PATRIOT Act of 2001 (update to 18 USC 1030)	2001	Defines stiffer penalties for prosecution of terrorist crimes
Accountability	Sarbanes Oxley Act of 2002 (SOX) or Public Company Accounting Reform and Investor Protection Act	2002	Enforces accountability for executives at publicly traded companies, this law is having ripple effects throughout the accounting, IT, and related units of many organizations
Spam	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN SPAM Act) (15 USC 7701 et seq.)	2003	Sets the first national standards for regulating the distribution of commercial email, the act includes mobile phone spam as well
Fraud with access devices	Fraud and Related Activity in Connection with Access Devices (18 USC 1029)	2004	Defines and formulates law to counter threats from counterfeit access devices (ID cards, credit cards, television equipment, mobile or electronic serial numbers, or the equipment that creates them)

Then copy product protection, identity theft, then in banking; in banking you find laws of the terrorism, stiffer penalties for prosecution terrorist crimes, accountability we have already discussed about this Sarbanes Oxley Sct or for computing public accounting reform.

Then the spam, so regarding pornography and other things fraud with access devices, so these are various, so what we find over here may be there are various laws with respect to data security and throughout like in different in countries, who started from way back in 1934. So, in Indian Parliament in 2000, the Information Act 2000 was enacted. The Information Technology Act was amended again in 2006. So, which replaced the old laws which were governing the post and telegraphs and it now reflects the new realities of the new information communication technology.

So, protection by the law; the IT Act offers the much needed legal frame work. So, the information is not denied, legal effect validity or enforceability solely on the ground that is on based on electronic records. It provides ways to deal with cybercrimes, in view of the growth and of transactions and communications carried out through electronic records, the act seeks to empower government departments to accept filling, creating and retention of official documents in the digital format.

The Act is also proposed a legal frame work for the authentication and origin of electronic records communication through digital signature. In E-commerce the

provisions of the act contain many positive aspects. The implication of these provisions of the E-business would be that, the e-mail would now be a valid a legal form of communication in our country that can be duly produced and approved in the court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital signatures; digital signatures have been given legal validity and sanction in the Act.

The act throws open the doors for entry of corporate companies in the business of being certifying authorities for issuing digital signature certificates. Notification; the Act now allows the government to issue notifications in the web, thus heralding e governance. Official communication, the Act enables the companies to file any form, application or any other document with any office authority or agency owned or controlled by the appropriate government in electronic forms. By means of such electronic form as may be prescribed by the appropriate government.

And information security; the IT act also addresses the important issues of information security which are very critical to the success of the electronic transactions. The act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of security procedures as stipulated by the government at a later date. So, these are some of the mentions which may find prominence in the information security Act and also we find the data protection has a major mention over here. So, either IT Act 2000, it is now possible for corporation to have a statutory remedy in case anyone breaks into their computer system or network and causes damages or copies data.

So, the remedy provided by the Act is in the form of monetary damages not exceeding rupees One Crore. So; however, we can understand that the law is not comprehensive. So, because it may so happen like when you are talking of who is responsible like if some stakeholder, some users have misused the internet for their personnel purposes and posted some data may be which becomes viral then, whom do we hold responsible for it? Those who have posted it or may be to the website that they have posted the owner of that portal, who is responsible? These type of questions becomes like ethical issues when we are dealing with the thing, who is responsible?

And there is because when we speak of internet we speak of another right which is side by side freedom of speech, so the freedom of expression. So, when these type of things are there corresponding ethical issues come regarding censorship in the internet. So, because there are no suppose more so in the case of globalization and may be the, where there is no territories and may be no government regulation. So, there or can debate can arise can government put censorship also to the information being shared and to what extent. So, the debate for there could be debate both for and against censorship, but and however, there are tools which are also getting developed, which can overcome any form of surveillance and banning of access.

So, on one side there are ethical questions regarding whether the surveillance should be done is it not, be creating a barrier for some of the rights which are like fundamental rights for the individuals and the other side it is giving rise to a new industry, new ways of finding out how this surveillance mechanisms and banning of access mechanisms can be bypassed and you can have access to the data. So, there are ethical issues with respect to these type of products also. So, they there could be issues with these type of products also.

So, first issue which becomes relevant in this case is that of having no territorial borders. So, for the internet actually there is no border except for the place where some of its use have been banned and. So, like with now with the advancement of technologies like where internet can be accessed from the mobile phones and all with the integration and the convergence of the technologies, this no territory concept has become more prominent in present days. So, next what we comes important is the smart censorship; in smart censorship more and more intelligent software programs are used to censor.

So, smart filter is one such software whose customers are ironically those who smother democracy by limiting the freedom of speech. So, the irony of the IT is that. So, it can be used as a weapon both for and against certain issues that you are representing. Unintended censorship, so these are several software programs like work as that work has net nanny's in educational institutions, workplaces and households. So, they try to block certain words as they match could be regarding pornographic words.

So, even some innocent words if they are matching some pornographic words they get blocked. So, when on one side these type of softwares are getting developed on the other

side there is a parallel way of development of some other softwares, who can circumvent this effect. So, now, there are softwares available, who can circumvent the net nanny's government bans and site blocking technologies. So, like proxy servers are private networks which are virtual private networks which can be subscribed to. So, there are other types of softwares which are called sneakernet, so when censors are busy in the virtual world to suppress things happening. So, it help like so like this sneakernet (Refer Time: 28:51) to carry data from one place to another and distributing it.

This needed no network at all. So, we can tell like censorship is justified on some basic moral grounds for may be the for the larger interest of the person, the citizens and the country often the greater interest of the organization, but also prudence have to be called for. So, that the peoples basic right for communication and freedom of expression are not hampered. So, like pornography if it is seen from its production aspect is a violation of human dignity because it uses persons as sexual objects.

Seen through my consequence it is a cultural and religious degradation, but when the minor see the sides and interact through them, its social repercussions are undesirable. So, the dilemma is that for what should be done in this case. Because all the adult materials then goes against the traditionally held moral values, but this is a hugely growing industry now. So, the people who live in this industry or who work in this industry are itself in a position of self doubt they feel more guilty than the customers.

So, there is an nature, there could be natural laws of one's self worth, self esteem by being object of sexual pleasure to so many people, anonymous people whom even we do not know about. So, these are ethical dilemmas then these type, this is just an example. So, these type of things what needs to be done in these cases and what are the steps taken. In what consequences we are, when you are trying to stop this things happening. Then what are the larger consequences that you are looking into and protection of which right we are looking into these needs to be well balanced.

In the next section we are going to deal with the examples of different crimes that are related to computers.

Thank you.