

Audio transcripts and lesson notes

Hello and welcome to the ISO 27001 Lead Implementer Training Program. I am Anup Narayanan, the instructor for this training program. Let us start with Chapter 1, The Importance of Information Security. In this chapter we shall look at why Information Security is important, first, from a personal perspective and then from a business perspective. The aim of this chapter is to set the foundation for the rest of the program.

Let us start by looking at the importance of Information Security in your personal life.

The following scenario is something that you would have experienced often in real life. Imagine that you are at a restaurant and after finishing your meal, you hand-over your credit card to the waiter. The waiter takes the card and returns it after charging the card. The whole process takes about 5 to 10 minutes. Have you ever asked yourself whether there is a possibility that the card could be misused during this time?

Now, ask yourself this question. “How much personal information do I have? What is the value of this personal information? And, how well am I protecting my personal information?”

Some examples of personal information are, credit card numbers, passport or social security numbers, emails and other correspondence, previous or current job records, medical or health care records, bank statements, financial statements and salary details. In fact, a lot of devious people would be seriously interested in getting their hands on your personal information.

In fact, there is an industry jargon for personal information and it is called PII, which stands for, Personally Identifiable Information. The people who intend to steal your personal information are called identity thieves. Statistics say that an individual’s PII is worth approximately \$610 on an average to an identity thief.

So, why will someone try to steal your information? As explained in the previous screen, your personal information is worth considerable money. So, money is the primary intention. Also, some of your personal information involves secrets that you do not want others to know. If an identity thief gets access to these secret data, you could be blackmailed, or worse, if they reveal these secrets, you could lose your reputation in the society, at the work place and in your family.

The end-result is severe mental trauma, financial strain and loss of reputation

So, you are now able to see that information has tremendous value and has the power to cause you severe discomfort if not protected properly. Hence, let us summarize as follows. Information exists in many forms, Information has a value and hence this information must be protected.

We shall now define the protection of information as “Information Security”. You will later see in this course that we use terms such as “Confidentiality, Integrity and Availability” to define information security. But, more about that later.

You have now understood the value of information security in your personal life. Let us now look at information security from the perspective of a business.

In this section, we shall explore the business importance of Information Security

Let us try to answer the question, “Why is Information Security important for a business?” In fact, during my information security interactions I come across this question often – “Is Information Security meant only for IT or Information Technology companies?” The answer is “NO”. Information Security is important for all organizations that have valuable information whether they are in the Information Technology or related businesses or not. In fact, even a Noodle Shop needs information security. Let us look at a case study.

Imagine that you are the proud owner of a noodle shop that you have named “Noodle 2000” and you are now getting into big business mode by franchising your business. Let us now look at the important business information around your noodle business.

The “Noodle 2000” business uses a lot of valuable business information for its operations and management. Some of them are, the sales figures, projections, business expansion plans, marketing strategies, prices at which raw materials such as chop sticks are purchased and the secret recipe of the noodles. In fact, when it comes to the price at which raw materials are purchased, you may be buying the same raw material from different suppliers at different prices. You do not want one supplier to know that you may be in fact paying him lesser than what you are paying the other supplier. Well, as you can see now, you would not want to disclose all this information as it would affect the way you do business and your business competence.

Now, who would be interested in getting their hands on this information? Without a doubt, your competitor, who is just waiting to launch a new brand, “Noodles 2001”.

Let us now summarize. A business depends on a lot of success factors such as quality of deliverables, on-time delivery etc. Along with this, you have seen that security of business information is very important. Business information includes customer data that you may handle and intellectual property and more. The business information could be compromised due to incidents or accidents that may happen knowingly or unknowingly. The ultimate impact is on customer trust, business sustenance & prosperity and ultimately employee livelihood.

Now, let us take a look at some of the different types of business information. We can broadly classify this into two, “Information that is produced by the business” and “Information that the business takes from others”. The first category, that is, “Information that is produced by the business” includes Business Intelligence, Financial Data, Source Codes, Designs, Documents, Product details etc. The second

category, that is, “Information that the business takes from others”, includes Information given by the customer, employee records etc.

Let us go a little more in-depth. Financial data is an example of information produced by the business. This is used for managing revenue and expenses, meeting regulatory requirements and for informing the share-holders about the financial health of the company. Disclosure of this information could lead to loss of competitive advantage and legal repercussions.

Another example of information produced by the business is “Business Intelligence” that is used for forecasting as well as for producing new services and products. Disclosure of this information may lead to loss of competitive advantage and subsequent loss of revenue and jobs.

Similarly source code and new product designs are valuable information that enables the business to produce new products and to become leaders in their specific market segment. Disclosure of this information could lead to loss of competitive advantage, loss of market share and revenue.

Let us now take a look at some of the information that the business takes from others’, especially from customers. In today’s outsourced business model, the customer often provides the business with important information such as product designs, source codes, financial data etc. Any disclosure of this information could lead to loss of customers, loss of reputation, money and the business could end up facing legal repercussions.

Another example of information taken by the business is employee records. Organizations typically store employee records that include health, personal and sometimes financial information. The business is responsible for protecting these records from unauthorized disclosure as disclosure of personal information could harm the individual considerably and we have seen this at the beginning of this video.

So! Now we have seen the importance of information for a business, examples of some types of information the business stores and processes and what could go wrong if this information is disclosed. Hence, there is a need to protect this information and this protection we term as information security.

Information Security for a business is required for the following reasons, 1 - to ensure that the organization stays in business, 2 - to grow in business and generate revenue, 3 - to preserve reputation and enhance it because good information security gives the organization a lot of credibility, 4 - to be on the right side of the law and 5 - to give confidence to customers, stake holders, employees, business partners and the government.

Now, we have seen why information security is important. But it is not so easy to implement a good information security management system in an organization or business. The reason is very simple! There is so much information, in different forms and in different places. It takes considerable effort to identify all these information and to protect it.

The first challenge is to understand the different forms in which information is stored. This includes Paper.

Electronic media such as CD's, USB Drives etc.

Hard disks and memory chips of computers and computing devices

And...even in the human mind?? Now, that's interesting isn't it?

So, the challenge is in controlling information in different forms and that too in different places.

The next challenge is in identifying the numerous ways in which information is stored and transmitted. As shown here, information stored in a computer can be transmitted through the internet as an email, the information can be printed on paper, stored in files in a cabinet or some of it could end up even in a trash can.

Another way in which information can flow is through verbal communication, where a human being talks about information which is stored in their minds to another individual who may choose to talk about it to others.

Hence, the big challenge is to identify the different pieces of information in an organization, find out how they are stored and transmitted, determine which information can be disclosed and cannot be disclosed and protect it from threats such as accidental deletion or destruction, fraudsters or hackers, competitors and even natural disasters.

Hence, the solution is a well defined Information Security Management System and that is what this whole training program is about. An Information Security Management System is often referred to as an ISMS. An ISMS uses a combination of technology and processes to protect business information as best as possible from relevant threats.

You will learn more about ISMS in the next chapter.

Thank you and please make sure that you go through all the available resources in the e-learning portal.