Part 1: introduction

Chapter 1: The meaning of security

**Definition**

Security architecture is about constructing information systems that are safe from attack.

A secure system is a system that conforms 3 principles of the information: confidentiality, availability, integrity

Any attacks that break one of the 3 principles will make the system not secure anymore.

There are many attacks that stops the system from being secure and here is the list

* SQL injection
* DDOS
* Zero-day attack
* XSS attack

**Business Risk**

* Assets are called things that have value in a business environment
* Business impact is when assets in business are damaged which is called threats
* We use a layer of protection to avoid threats happening
* The process of identifying business assets, recognizing threats, assessing level of business impact that would be suffered if the threats were to happen, analyzing the vulnerabilities is known as operational risk assessment.

**Risk Management**

We cannot do business without taking risks, to gain revenues and money, we need to take risks.

If we decrease this risk, other risks will increase, therefore we must conduct the risk management to have a broad view of our risk.

The question is how much risk? It depends on the size of the risks, the potential costs and gains

The aim of risk management is to balance the various risks between costs, risk and revenue

Risk management comprise risk assessment and risk mitigation

Conducting risk assessment will result in a document that describes all the business assets, dangerous threats and vulnerabilities.

Conducting risk mitigation will result in a document that assesses level of business impact and level of controls in order to apply assesses level of business impact and level of controls into our organization

We must conduct risk management first in order to analyze business and security requirements ranked in order of priority as a series of control objectives –abstract description of business requirements before constructing the security architecture.

Here are some business risks that are very likely to occur to any company:

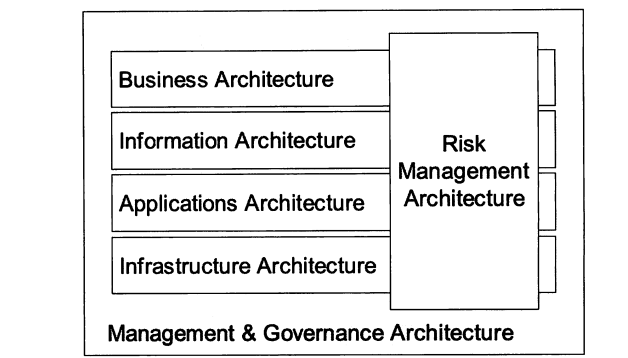
* Disclosure of personal information such as bank account, medical records and so on
* Fraudulent buyers and sellers
* Systems failed and hence do not work properly and did not maintain availability for users to access

Chapter 2: The meaning of Architecture

For example, the Sydney Opera House is the most well-known example of a modern architecture, this modern architecture acts as a **broad view- an overall concept** which means that when each component of the architecture is building, it has to base on **this overall concept architecture** to build rather than create its own ideas to build. Therefore, this overall concept architecture can break down into manageable pieces which makes it easier to integrate after completion.

Building an architecture helps us to manage complexity successfully. A small project does not need architecture because their level of complexity is limited. But when the size and complexity of a project grows, we need an architecture to break down complexity into apparent simplicity.

An example of an information system has some sub-architectures:



The top layer is business architecture

The lower layer is information architecture and application architecture and infrastructure architecture

The application architecture are the computer programs and the modern application architecture are: service-oriented architecture, distributed system and so on

Infrastructure architecture include: the computer platforms (hardware and Operating system) and computer network (cables, routers, etc.)

The software that connects infrastructure and application is commonly known as “middleware”.

Imagine a checklist that has the following items: engine block, pistons, piston rings, piston rods, bearings, valves, cam shaft, wheels, chassis, body, seats, steering wheel, gearbox, etc. Suppose this list is every component we need to build a car. If we go through the checklist and make sure we all have these components, does it mean you have a car? Not exactly.

A car is a good example of a complex system. It has many sub-systems and building and designing a car need a system engineering approach the same with building enterprise security architecture.

Summary:

Building a security architecture needs a holistic/system engineering approach.

Architecture means taking a holistic, broad view approach by which the system will be designed and built.

The purpose of the architecture is to ensure the consistency of the overall view and break up the complexity so as to present greater simplicity and make the overall view easier to implement.

Chapter 13: Component security architecture

Component security architecture is a tradesman view about detailed standardized data structures for protocols.

The purpose of this component layer is to achieve integration among components that have compatible interfaces to support integration and inter-operability. We need to set up so that the compliance standards component can exchange in an agreed precisely way on protocol communication.

This chapter discuss standard security such as ISO W3C, IEEE, ANSI, etc.

And talks about protocol stacks http/https, ssl, tls, ipsec and etc.