# System Security Handbook

t1mgit

2023

# Contents

# Chapter 1

# Introduction

## 1.1 Purpose of this book

This book is NOT a complete and organised text on security. This book IS a sampling of guide notes and reference material collected (and still collecting) whilst studying and working in the security domain. This book is not intended as the be-all and end-all of security but more akin to an identifier of key topics for which additional information should be sought elsewhere. This book does intend (eventually) to discuss the kinds of things one should think about when implement security into a system.

## 1.2 What is security

Most security text books will tell you that 'Security' is about maintaining the three pillars of 'Integrity', 'Availability' and 'Confidentiality'. [1] While this is true, the implementation of security processes, procedures and tools inline with "good practise" can make a system cumbersome or impractical for the end user. In a similar vein, implementing security has additional costs (money, time etc.) which could, if security is poorly planned, be unnecessarily excessive. Therefore the art of security is finding a solution that not only optimises the three pillars of security but also the end users budget and operability of the system being secured.

[1] Insert reference for this first line

## 1.3 What to to expect

Before getting bogged down in what kind security technologies should considered, the system being secured must first be understood. Subsequent to that, the threats, probabilities and risks faced the system must be identified and a risk reduction method selected. This will be the subject of the first two chapters. Subsequent chapters will essentially list and briefly describe various methods and tools used in securing a system.

# Chapter 2

# What is a system

# Chapter 3

# Security Risk Management

## 3.1 What is Risk Management?

In brief, Risk Management is about identifying threats (or hazards) directed toward the business, then quantifying both the impact and likelihood of the threat occurring.

Safety risk management is well understood and practised particularly in more dangerous industries such as construction and mining. It also has government backing with Work and Safety legislation.

Shown in Figure 3.1, ISO30001:2018 is a popular international standard for risk management. It defines the following risk management process:

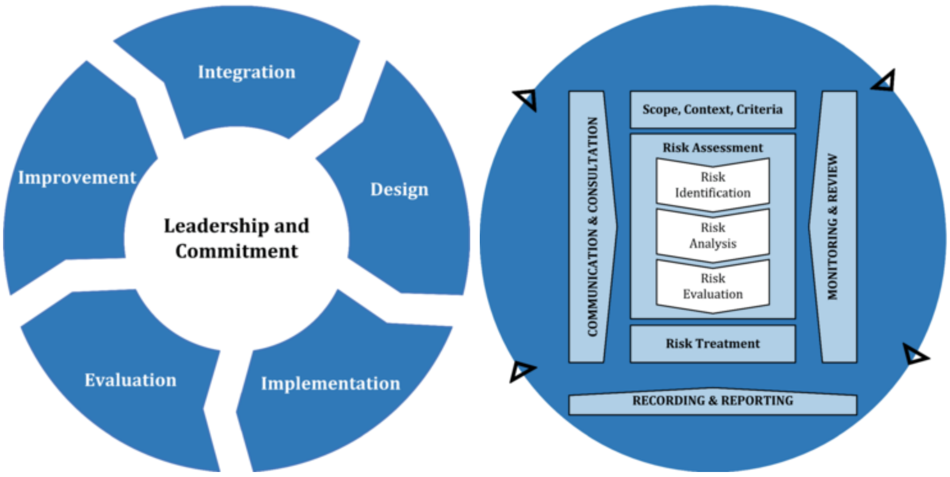

Figure 3.1: Risk Management Framework and Process

- Communication;

- Defining Risk;
- Risk Assessment;
- Risk Treatment;
- Monitoring and Review;
- Recording and Reporting.

## 3.2 Communication

The objective of Communication is twofold. First it is an exchange of timely and accurate information with and between relevant internal and external stakeholders. Second it promotes an understanding of risk and how it is used as the basis for decision making prosecuting actions.

## 3.3 Defining Risk

The Risk Management program should define the organisational level applied to the risk management objectives e.g. Strategic, Program, Project, Operational. Scope requires consideration of: a)Objectives and outcomes; b)Resources and responsibilities; c)Tools and techniques; d)Record keeping.

Furthermore, the program needs to define the method of risk evaluation. A simple example follows:

- **Define Impact***

  *Includes reputation damage resulting in financial loss

  Low=Financial loss less than 1 year earnings

  High=Financial loss more than 1 year earnings

- **Define Likelihood**

  Infrequent=Occurs less than once per year

  Often=Occurs more than once per year

| *Risk Table* | **Low Impact** | **High Impact** |
|---|---|---|
| **Occurs Infrequently** | Low Risk | Medium Risk |
| **Occurs Often** | Medium Risk | High Risk |

The example above defines consequences (Financial and reputational loss) and a quantifiable risk level (annual earnings). A larger risk definition will consider the organisations context - that is the wider external and internal factors within the operating environment. This is sometimes referred to as "Threat Surface". Finally, a risk management program needs to define the appetite for risk. How much risk is acceptable before the manage should pass the decision to act (or not act) to a higher authority.

## 3.4 Risk Assessment

Assessing risk encompasses the three processes of:

- Identifying the risk source: Where does it come from? Where are we vulnerable? What is the threat environment?

| **Tangible Risk Source** | **Intangible Risk Source** |
|---|---|
| (Loss of) physical assets, including data or information asset stored computer disks.<br>Also, negligent damage to third party assets including environment, property and people.<br>Capability gaps.<br>Change in operating environment and/or external events. | Usually socio-economic or legal risk which may impede achieving the objective. E.g. Public opposition could lower reputation and result in boycot, or legal actions.<br>Knowledge gaps.<br>Change in operating context. |

- Determine the consequences if risk materialises: What will happen? How bad will it be? How likely is it? Are there any mitigating factors (controls)?

- Evaluation: Compare the assessed level of risk against the organisations risk thresholds to inform the decision to act (or not) and the amount of effort or resource put to mitigating the risk.

## 3.5 Risk Treatment

## 3.6 Monitoring and Review

## 3.7 Recording and Reporting

# Chapter 4

# Physical Layer Security

The concern of physical security is preventing unauthorised access to those tangible assets which process, transform, manipulate data and information. In the IT world such assets may be computer terminals, network servers, switches, cabling etc. Electrical power supplies needed to run the network are also physical assets. Automated industry may additionally include various machines, device controllers and environment sensors. Hard-copy or paper documents should not be discounted when considering physical security.

In this section discussion shall focus on the physical layer referred to by the OSI or TCP/IP networking model. This is the physical medium that carries the information, as well as the connection devices.

## 4.1 Physical Access to Hardware

## 4.2 Remote Intercept of the Physical Layer

Here we refer explicitly to the detection of information signals outside of the intended information boundary.

Consider an argument occurring in a block of flats. It is likely that the intended information boundaries are the walls of the single flat in which the argument occurs. However, the argument is heard in surrounding flats because the sound vibrations are conducted (although damped) through the walls. Thus information has been received without being ”present” in the argument.

In current practise information may transmitted using methods concerning electromagnetic radiation or mechanical vibration - the transfer of energy as a wave of vibrating particles within a medium.

### 4.2.1 Electromagnetic Radiation

Information can be transmitted as energy in the electromagnetic spectrum which includes:

- Visible light;
- Infrared light and thermal frequencies;
- Ultraviolet and radio frequencies.

Electromagnetic radiation my be deliberately employed to transmit without wires over large distances. Radio is a prime example. However most high-school physics textbook explain that an electrical charge travelling with a velocity creates a magnetic field, or a conductor carrying a current creates a magnetic field perpendicular to the direction of current flow. The fundamental principle of radio enginering is: "A single unshielded conductor with internal resistance and carrying an alternating current will radiate energy as electromagnetic waves".[1] Therefore, if it is possible to detect the radiated energy and information leak may exist.

### 4.2.2 Mechanical Energy

Information can be transmitted through a medium as energy characterised by particle vibration travelling as waves through the medium. Audible sound in air is a well understood example. Solids, Liquids and gasses all can transmit vibration however the effectiveness is highly specific to precise conditions of the medium. In general terms, a stiffer the medium will absorb less energy and is therefore a better conductor.

[1] Bailey, D., Practical Radio Engineering and Telemetry for industry, p2