

MAKING  
SENSE  
OF  
SECURITY

---

*Corporate Edition*





# MAKING SENSE OF SECURITY

---

*...security of a corporation involves planning for and finding the best strategies to avoid situations that might threaten the company or business continuity.*

---

*'Tunde Asaaju*

Making Sense of Security

Copyright © 2021 by Tunde Asaju

All rights reserved under International Copyright Law. Contents and/or cover may not be reproduced, stored in a retrieval system, or transmitted in whole or in part in any form, or by any means – electronic, mechanical, photocopying, recording, or otherwise – except for brief quotations in printed reviews, without the express written consent of the publisher.

Hard cover ISBN: 978-978-99366-9-4

Executive Edition | First printed in June 2021

This edition is NOT FOR SALE

For worldwide distribution

Cover design and text layout by  
Dayo Eniola-Collins | [dayocolins@gmail.com](mailto:dayocolins@gmail.com)

Published and produced in Nigeria by  
ECHORDmedia





# CONTENTS

Dedication .....	vii
Acknowledgement .....	ix
The Author .....	xiii
Introduction .....	xv
<b>Section 1   About Security .....</b>	<b>1</b>
<b>Section 2   Risk Intelligence .....</b>	<b>11</b>
<b>Section 3   The Three Pillars .....</b>	<b>27</b>
<b>Section 4   Physical Security Technology .....</b>	<b>61</b>
<b>Section 5   IT Security .....</b>	<b>113</b>
<b>Section 6   Data Analysis .....</b>	<b>137</b>
<b>Section 7   Safety Vs. Security .....</b>	<b>159</b>
<b>Section 8   Security-By-Design Principles .....</b>	<b>175</b>
References .....	250





# DEDICATION

*To  
Agatha, Kendra and Kevin*





# ACKNOWLEDGEMENT

**P**utting together a book is harder than I thought and more rewarding than I could have ever imagined. None of this would have been possible without God's grace to be alive. All glory to God! I have to start by thanking my awesome wife, Agatha for her moral support and early reading of the preface draft for correction and advice. Thank you so much, darling.

In this book I have synthesized many fields of knowledge and years of experience working as a risk

manager, as well as extant research on enterprise risk strategy, technology innovations and businesses. I had (even up till this moment) privilege of working very closely with various great think tank personalities and visionaries (business executives) that provided tough opportunities for my potentials development. These experiences have shaped major portions of this book. I thank all the executives and directors of Sahara Power Group especially Mr. Tope Shonubi who gave me the benefit of the doubt, who trusted me and confided in me and also extended that trust to the people who work with me.

I have drawn on many streams of strategic thinking, managerial practices, and developments in academia and industry. I have benefited greatly from the practical teachings and leadership of best minds in private and corporate security managements: Tunde Soluade, Deji Bamgbose, David Creswell and Mike Igbodipe, with whom I have shared a long journey of intellectual and professional development.

I am very grateful to Capt. Deji Bamgbose (Rtd) who took his precious time while on vacation abroad to review the entire book manuscript. Special thanks go to Col. Tunde Soluade (Rtd) who brought me on as just a Technical Security Officer at his company and then allowed me to rise through the ranks to become Technical Security Consultant of the company within three (3) years. Thank you for introducing me to



security technology and company culture.

In addition, several academics, risk professionals and leaders' thoughts are great integral part of this book. Big thanks to: David Creswell (International Security Management Institute), Science Direct Journal, Parker D B (Computer Security Management), Halkyn Consulting Security & Risk Management and so many others.

I want to thank 'Dayo Eniola-Collins and Mary-Gloria Anyanwu, who really pushed the manuscript's quality and contents in very profound ways.

Finally, to all those who have been a part of my getting here from my parents to all my good friends and colleagues, I will like to say “**Big Thank You**”.





---

## THE AUTHOR

**B**abatunde Asaaju is a certified Security Risk Management Professional and Data Analyst, with more than 16years experience in industrial security and safety. He holds MBA in Security Management (Forensic Intelligence Specialization) at Babcock University and first degree in Electrical and Electronic Engineering with various other post graduate/professional certifications in both security and safety.



The long list of his qualification includes but not limited to; Level 6 Diploma (PGD) in Security Management with ISMI, UK; Post Graduate Certificate in Data Science and Business Analytics at the University of Texas at Austin, USA; Post Graduate Certificate in Project Management at University of Lagos; Information Technology, CompTIA Security+; NEBOSH IGC Certificate in Occupational Health and Safety; Certification in Physical Security Technology with Reditron, South Africa. He is an international member with; American Society Industrial Security (ASIS) and International Security Management Institute (ISMI) and a fellow member with; Institute of Criminology and Strategic Studies (ICSS); and The Institute of Management Consultant (IMC).

Babatunde has realized a big gap in corporate security practices due to stakeholders' indeterminate perception and mindset that simply requires paradigm shift. ***“Making Sense of Security”*** is the product of his strong expansive years of experience as a result-oriented Manager and Consultant in risk-informed and data-driven corporate security management with various private security outfits and multinational organisation.



# INTRODUCTION

*Paradigm shift in corporate security consciousness; **the urgent need!***

**A** couple of years ago even up till now in some organisations, the issue of security in a corporate environment is mere having a guard at the facility or building entrance for gate control and possibly monitors who/what goes in or comes out of the company. And as such, corporate security has been dominated by a '**defensive**' approach, focused on

protection and loss prevention (traditional security). The head of security is seen as little more than the '**guard at the gate**', someone whose actions invariably impede people's activities instead of enabling the business to function more effectively. Typically, heads of security came from a national defense pool, namely police, armed forces or intelligence. There are many reasons companies tend to recruit security managers from these backgrounds which are outside the corporate security functions, most times. And these traditional security skills are associated with an approach where security is perceived as a '**dis-enabler**' of business because the professionals with only formal security training can tend to be risk averse mainly, while businesses need to take calculated risks to stay ahead of competitors, break into new markets and maximize profits.

Security function in this age of globalization means a proficiency of planning for and finding the best strategies to identify and effectively mitigate or manage situations that may threaten the existence of any establishment. With the fast changing global landscape shifting the structure and pace of corporate life, both in the way businesses operate and the environments they work in, security risks are ever more complex. Many of the threats, such as acts of sabotage, organized crimes (internal and external) and cybersecurity, are asymmetric and networked, making corporate security



more difficult to manage with just a “**defensive**” or traditional approach.

Corporate security or lack of it – can greatly impact an organisation's bottom line and reputation, there is every reason to argue that it should be high up on every business owners' agenda. In its wider context, corporate security identifies and effectively mitigates or manages, at an early stage, any developments that may threaten the resilience and continued survival of an organisation and its most valuable assets. Corporate security should not be seen as a standalone function, but be recognized as having the ability to work with and enhance other areas of the business such as corporate governance, business continuity, corporate social responsibility, regulation, and overall safety assurance. Security strategies, procedures, protocols and technologies must be developed to ensure close coordination of all functions within the organisation that are concerned with security, continuity and safety.

Unfortunately, some organisations are yet to appreciate how essential the role of corporate security can be to the success of their business sustainability which requires a paradigm shift in security from simply protecting companies to being the source of competitive advantage due to lack of the actual trust and right understanding. The most painful part is that many security professionals face challenges convincing

senior managements or boards on the great importance of security to business development. The core challenge lies in managing to appropriately match security principles and philosophies with profit-oriented enterprise perspective.

“**MAKING SENSE OF SECURITY**” is a book intended for both security practitioners and business executives longing to align corporate security functions with the company strategies for successful attainment of business performance goals in a cost effective manner. Businesses must orient their “**Security**” with the below key areas in order to be a success;

- Board Agenda
- HR & HSE Management
- Operations/Third Party Supply Chain

The concept of the handbook relies on comprehensive and practical definition of security as a function of crime prevention to asset protection through data analytics (data) and risk-driven business resiliency.



*Key information*

*Mathematically;*

*Security = Crime Prevention + Asset Protection + Resilience.*

Section

1

# ABOUT SECURITY



*If one sets out to think about security, an obvious starting point might be to ask: what is security anyway? Can security reality be the same as its perception?*

*In all areas of life, definitions constitute the bases for action. And of course, the conditions of some terms can become insufficient, or even confusing, if they retain their traditional meaning. In such cases, the attempt to apply the old definitions to the changed character of the world may reveal their limitations. The term “security” seems to be such a case.*



MAKING SENSE OF SECURITY

---





# SECURITY

## *What does it mean?*

**T**he fundamental challenge facing security as a profession or service is the **MISCONCEPTION** about security among many people. The general perception is that security is about “**guards, barriers and guns**”.



*Key information*

*But all of these offer only a false sense of security.*

Even some security professionals do little to dispel this

perception as it may be suited to their comfort zone, or it may be what they practiced as a career.

It is important to be mindful of the above when considering defining or designing security and its architecture. All too easily, we can slip into a mindset that reinforces these general preconceptions that security is about restrictions, curtailing freedoms, controls and obstacles. And none of which are conducive to healthy living and business growth.

That, however, is physical security at its most basic – in effect; the guarding function is just to attain security not security in itself.



*Key information*

**Security should always be viewed as a business/living enabler.**

## What is Security?

The word security is derived from '**secura**' a Latin word meaning *se (without)* and *cura (care or concern)*.

### Dictionary definitions:

- *State of well-being*
- *Freedom from fear of uncertainty, danger, risk etc.*
- *Freedom from apprehension or doubt; well-founded confidence*
- *Freedom from financial cares or from want*
- *Something that secures or makes safe; protection,*



*defense*

- *Precautions taken to guard against theft, sabotage, stealing of proprietary secrets etc.*
- *Something given or deposited as surety for the fulfillment of a promise or an obligation*

This was succinctly expressed thousands of years ago by ancient Greek Philosopher, Thucydides who wrote that: *“The security of the city depends less on the strength of its fortifications than on the state of mind of its inhabitants”*.

Meanwhile, freedom in a real sense is about being vulnerable to one another, realizing that our ability to connect is more important than feeling secure.

In a world of perceived uncertainty and danger, the desire for security becomes a central concern of political thoughts and personal actions. Against the threatening forces of unpredictability, rapid transformation and complexity, it appears to focus on longing for greater reliability, stability and tangibility that seems never to be achieved in reality.

While these form a traditional perspective, today security involves protection from unwarranted interference of:

1. Physical Assets
2. Human Resource Assets
3. IT Assets

## Incomprehensible, **WHAT SECURES NEEDS TO BE SECURED!**



### *Key information*

There is an old Latin idiom; **nemo dat quod non habet**, essentially this translates as, '*you can't give what you don't have.*'

This saying has fundamental ramifications for provision of SECURITY which means that a security provider must first possess SECURITY which is as well from one SECURITY to another SECURITY and so on. Isn't that incomprehensible? No wonder, a Holy Book states that “*...unless the LORD watches over the city, the watchmen stand guard in vain*”. *Psalm 127:1*

Can we then say security does not exist considering its dependency?

## The Science of Security

Analytically, however, the term “*security*” does not itself possess any stable or consensual meaning. Rather, it marks the perimeters of a highly contested terrain for;

- How is security to be achieved?
- Who/what is to be secured and against which dangers?
- What exactly to be provided to guarantee the required safety?

If one sets out to think about security in a real sense, an obvious starting point might be to ask: what is security anyway? Constituting such question may cause one to view security as an actual condition of existence that is independent of its affirmation in day-to-day discourse.

This ontological condition of security has been imagined in quite different ways by realism and idealism in international relations theory;

- **Realism:** *A relative condition in the present.*
- **Idealism:** *An absolute condition of the future.*

However, referencing security in both cases sought to signify certain objectivity. This way of thinking has had at least two implications for the way we ought to go about defining it.



*Key information*

**1st: Security is conceived as something that can be objectively known and thus needs to be diligently measured, monitored and improved upon by means of reason and scientific inquiry.**

**2nd: Security attains a normative quality: it appears as a good thing we ought to actively aspire to.**

From such a perspective, the general definition of security is usually thought to be encountered in the **absence** or at least **low** probability of **THREATS** to a certain thing (living/non-living).

## Logical ways of approaching SECURITY

<i>Essence of Security</i>	<ul style="list-style-type: none"> <li>● <i>Objective condition described by the absence or low probability of threats to a certain object.</i></li> </ul>
<i>Concept of Security</i>	<ul style="list-style-type: none"> <li>● <i>Who/what is to be secured?</i></li> <li>● <i>Which values are to be secured?</i></li> </ul>
<i>Governance of Security</i>	<ul style="list-style-type: none"> <li>● <i>What are the threats to security?</i></li> <li>● <i>By which means/strategies is security to be achieved and to what extent?</i></li> <li>● <i>How much resources should be devoted to security?</i></li> <li>● <i>Who is to do the securing?</i></li> </ul>

## Inference



### Key information

*Security is the combination of measures and resources, human and material aimed at securing an asset or activity from unlawful intervention.*

It is the implementation of a set of logical and systematic procedures and processes that when taken as a whole have the effect of altering the ratio of undesirable events to total events and a realistic plan of action to deal with major occurrences when preventive measures fail due to variety of practical reasons.

**Security**, thus is both

- A process of activity and
- A condition resulting from such activity

### Security Essentials

- A continuous activity
- A vital input in the system
- Both preventive & protective
- Which is not completely fool proof
- With an acceptable level of residual risk
- Striking a balance between security & facilitation

Security can be graded in three levels depending on the threat;

1. **Low Level** – To impede, detect and assess unauthorized external and internal activity
2. **Medium Level** – To forecast, Impede, detect, assess and neutralize external and internal threats
3. **High Level** – To facilitate complete protection including contingency / disaster management plan



*Key information*

Taking all the above viewpoints into account, a comprehensive definition of security could be *“a real, or perceived, state when there are no threats, or when existing threats do not pose a danger to the considered object.”*

Analytically, security is a function of crime prevention to asset protection through data analytics (data) and risk-driven business resiliency.

***Security = Crime Prevention + Asset Protection + Resilience***



Section

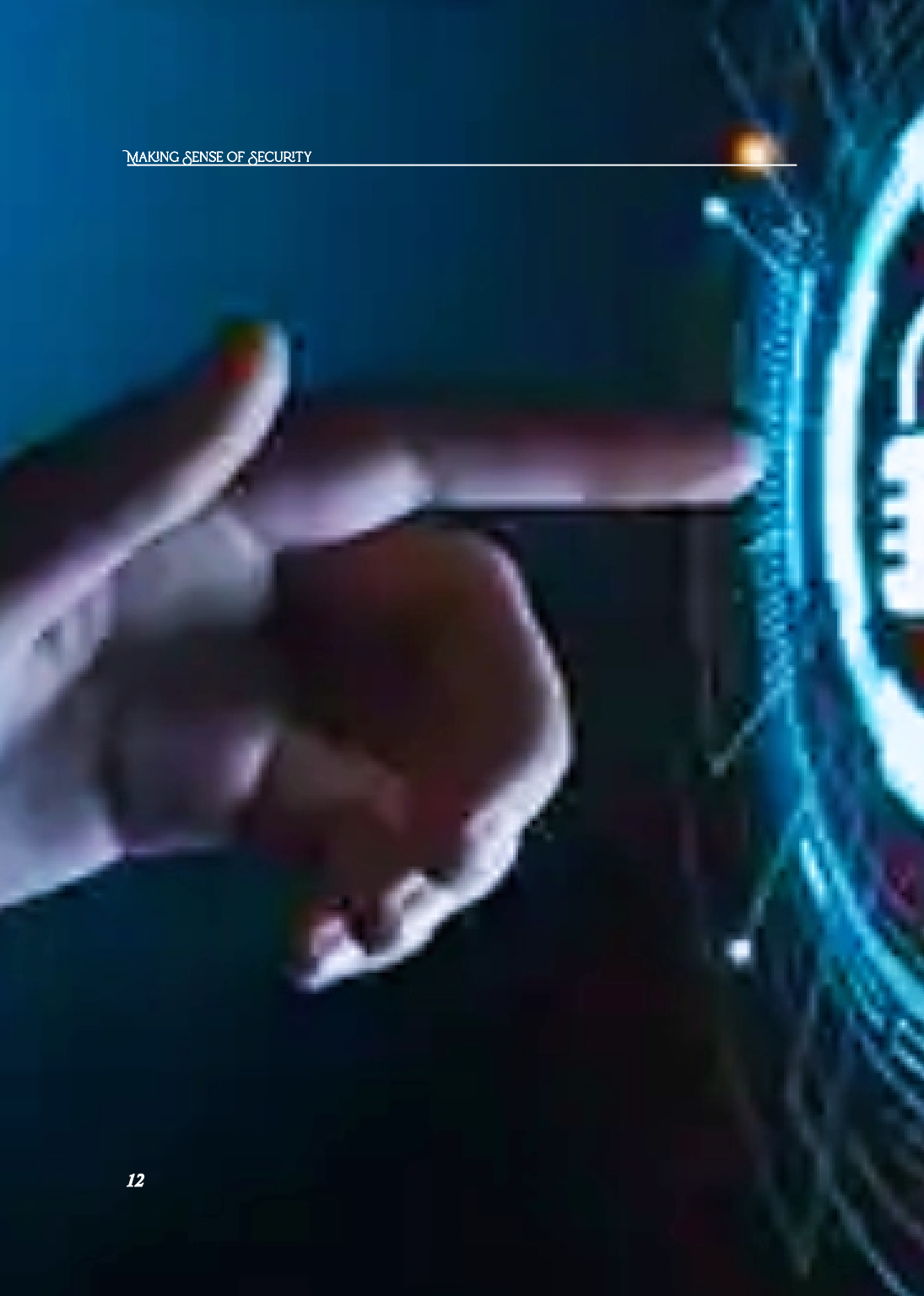
# 2

## RISK INTELLIGENCE



*Foundation is the first part of any construction and it must be strong enough to support the load of the entire building. It may seem like a simple part of the overall construction process, but your FOUNDATION is the most IMPORTANT part of your entire project.*

*This section contains ingredients or fundamentals for developing good security skills and techniques.*



# THE KEY INGREDIENTS OF SECURITY



**R**isk, Threat and Vulnerability are the most commonly mixed up important terms which are key drivers for determining **Security**. While it might be unreasonable to expect those outside the security industry to understand the differences, more often than not, many in the business or profession use these terms incorrectly or interchangeably.



### Key information

*Understanding the difference between threats, vulnerabilities, and risk is the first step because they form the basis for security metrics. What cannot be measured cannot be managed.*

This is a commonly accepted business paradigm, yet its acceptance within the security profession is not as far reaching as in other practices.

Simply put, data driven security refers to using measurable factors to design **protection system**. Thus, security metrics assist security professionals in making asset protection decisions through the measurement of performance based characteristics of the key drivers.

## Asset

*An asset is a resource of value requiring protection.*

An asset is basically anything of value. Assets could be abstract assets (*like processes or reputation*), virtual assets (*data*) physical assets (*building, a piece of equipment*), human resources, money, et cetera.

Asset value is determined by considering the following three elements:

- The criticality of the asset for its user and/or others
- How easily the asset can be replaced

- Some measure of the asset's relative value

### **Company Assets: *People, Property and Information.***

People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

### **Assets Management Process**

- **Step 1:** *Define and classify the assets*
- **Step 2:** *Rank the assets in order of importance*
- **Step 3:** *Create a profile for each asset*
- **Step 4:** *Manage life cycles of the assets.*

### **Threat**

*Threat is anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Threat could be actual, conceptual or inherent.*

A threat is any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It is also important to understand “*who are the people with the intent to cause harm*”.

A threat is what to be protected against. Since the dawn

of time, there have always been threats to security that manifest in many different ways. As long as there is something that needs to be protected, it goes without saying that there is something that you are protecting it from.



#### Key information

*Taking into consideration the uncertain nature of security and related concerns, with regard to creating a sufficient definition, it would be true to say that the only indicators, or measures, of security are particular “threats”.*

**Threat** – A criminal or terrorist event which can have negative consequences on a critical asset. Critical assets can typically be put into several categories:

- People
- Property or Monetary
- Continuity of Operations
- Intellectual Property
- Reputation

### Threat Components

- **Adversary/Agent** – Criminals, Terrorist, Disgruntled Employee
- **Capability** – Resources (education and training, facilities, methods)
- **Inhibitor** – Fear of Failure, fear of capture, public perception, law enforcement activity,

cost of participation.

- **Motivator** – Political, Religion, Personal Gain, Secular
- **Catalyst** – Events, Technology Advancement, Personal Circumstances

*Why do you think padlocks have been around for such a long time?*

Physical security threats used to be the most prevalent threats because that was all society was accustomed too. One can basically say that security threats are a part of life, but this doesn't mean you have to constantly live in fear of them.

After identifying asset value, the next step in a security risk analysis process is to conduct a threat assessment wherein the threats are identified, defined, and quantified.

## **Threat Assessment**

A threat assessment is a continual process of compiling and examining all available information concerning potential threats. It can be broken down into two processes;

1. Defining threats
2. Identifying threat event profiles and tactics

## Vulnerability

It could be referred to as weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

Vulnerability is a weakness or gap in our protection efforts.

### Types:

- Physical
- Operational
- Natural
- Human
- Technical

It is important to understand that vulnerabilities enable risk. Threats will always exist, and an organization or other entity will innately have value, but vulnerabilities are those that create the inevitable compromise of value.



### Key information

*In short, a threat may exist, but if there are no vulnerabilities for the threat to exploit, then there would be no risk.*

Threats are entities and they cause no harm on their own.



## Vulnerability Assessment

A vulnerability assessment is an attempt to discover and demonstrate weaknesses in a security device, system, or program. It is a process of identifying, evaluating, and classifying security vulnerabilities based on the risk they present to your enterprise, so that you can narrow down to the most threatening ones for timely risk reduction.



### Key information

*Every effective security practice is built on a strong foundation of policies and procedures, and the vulnerability assessment process should be no exception.*

## Key concepts of vulnerability assessment



Performing a vulnerability assessment can provide an accurate “**point-in-time**” representation of the organization's security posture.

## Risk

Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

**RISK = ASSET \* THREAT \* VULNERABILITY**



*Key information*

*Risk is a function of threat exploiting vulnerability to impact asset. Thus, threat may exist, but if there are no vulnerabilities then there is little or no risk.*

Similarly, vulnerability can exist, but if no threat then, there would be little or no risk.

Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to assets.

**Security Risk** is a function of;

- Consequences of a successful attack against an asset and
- Likelihood of a successful attack against an asset

**Likelihood** is a function of;

- The **Attractiveness** to the adversary of the asset
- The degree of **Threat** posed by the adversary, and
- The degree of **Vulnerability** of the asset

## Risk Management

The risk management process is a framework for the actions that need to be taken.

There are four basic steps that are taken to manage risk; these steps are referred to as the risk management process.



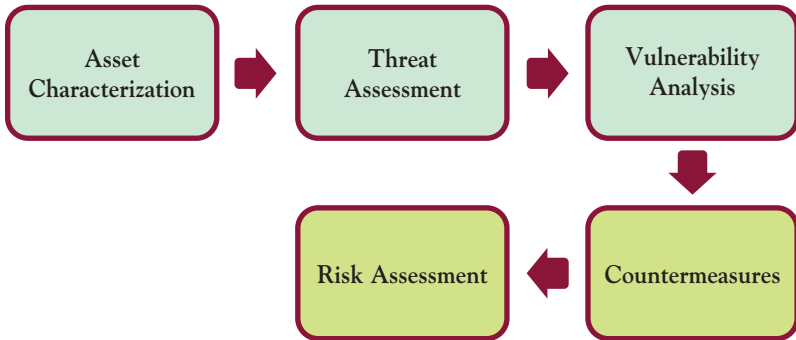
## Response to risks

- **Avoidance**
- **Mitigation**
- **Acceptance**

## Security Vulnerability Assessment Methodology

The SVA process is a risk-based and performance-based methodology.

Below is a standard 5-step approach;



Risk management is a central concept in the fields of security as **crime/loss prevention and asset protection** that helps to conserve the limited resources, apply the right solutions in the right places, and keep up with the changes in the operational environment.

### General Framework: Security Risk Assessment

1. **Understand the organization and identify the people and assets at risk.**

Understanding of organization in terms of hours of operation; types of clients served; nature of the business activity; types of services provided or products produced, manufactured, stored, or

otherwise supplied; the competitive nature of the industry; the sensitivity of information; the corporate culture; the perception of risk tolerance; and so on.

People include directors, employees, customers, visitors, vendors, patients, guests, passengers, tenants, contract employees, and any other persons who are lawfully present on the property being assessed.

Property includes real estate, land and buildings, facilities; tangible property. It also includes the “**goodwill**” or reputation of an enterprise that could be harmed by a loss risk event

## **2. Specify loss risk events/vulnerabilities.**

Loss risk events can fall into three distinct categories: crimes, non-criminal events such as human-made or natural disasters, and consequential events caused by an enterprise's relationship with another organization, when the latter organization's poor or negative reputation adversely affects the enterprise.

## **3. Establish the probability of loss risk and frequency of events**

Probability of loss (not based upon mathematical certainty) is a consideration of the likelihood that a loss risk event may occur in the future, based upon

historical data at the site, the history of like events at similar enterprises, the nature of the neighborhood, immediate vicinity, overall geographical location, political and social conditions, and changes in the economy, as well as other factors that may affect probability.

For example, an enterprise located in a flood zone or coastal area may have a higher probability for flooding and hurricanes than an enterprise located inland and away from water.

#### 4. **Determine the impact of the event.**

All the potential costs, direct and indirect, financial, psychological, and other hidden or less obvious ways in which a loss risk event impacts an enterprise should be considered.

**Direct costs may include:** Financial losses associated with the event, such as the value of goods lost or stolen. Increased insurance premiums for several years after a major loss. Deductible expenses on insurance coverage.

**Indirect costs may include:** Negative media coverage. Long-term negative consumer perception (e.g. that a certain business location is unsafe). Additional public relations costs to overcome poor image problems.

## **5. Develop options to mitigate risks.**

Options include security measures available to reduce the risk of the event. Equipment or hardware, policies and procedures, management practices, and staffing are the general categories of security-related options.

However, there are other options, including transferring the financial risk of loss through insurance coverage or contract terms (e.g., indemnification clauses in security services contracts), or simply accepting the risk as a cost of doing business. Any strategy or option chosen still must be evaluated in terms of availability, affordability, and feasibility of application to the enterprise's operation.

## **6. Study the feasibility of implementation of options.**

The practical considerations of each option or strategy should be taken into account at this stage of the security risk assessment. While financial cost is often a factor, one of the more common considerations is whether the strategy will interfere substantially with the operation of the enterprise. Take for instance; retail stores suffer varying degrees of loss from the shoplifting of goods. One

possible “strategy” could be to close the store and keep out the shoplifters. In this simple example, such a solution is not feasible because the store also would be keeping out legitimate customers and would go out of business.

## **7. Perform a cost/benefit analysis.**

The final step in conducting a security risk analysis is consideration of the cost versus benefit of a given security strategy. The security practitioner should determine what the actual costs are of the implementation of a program and weigh those costs against the impact of the loss, financially or otherwise.



Section

# 3

## THE THREE PILLARS



*A sustainable security plan or structure has three defining strategic thrusts; starting from prevention and protection to being able to withstand any eventualities (Murphy's Law states that; "if anything can go wrong, it will).*

MAKING SENSE OF SECURITY



# SECURITY AS CRIME PREVENTION



**T**his security approach seeks to prevent threats from arising in the first place by addressing the underlying causes that generate them before they emerge.

It is a reality that crime occurs every day. Regardless of the improved security efforts, crime still affects everyone at different place and time. Therefore, taking charge of personal safety is another sure reality that must be embraced at all time so as to avoid becoming a victim of crime.

## What is Crime?



### Key information

*There is no universally agreed definition of what a crime is. However, the most straightforward way of thinking about crime is to look at it in terms of a legalistic perspective – Crime is defined as an act committed or omitted in violation of an order into an offence.*

Crime can be classified as either **Acquisitive Crime** (*acts of dishonesty; theft and fraud*) or/and **Expressive Crime** (*acts of criminal damage, violence, terrorism, etc*).

## The Drivers of Crime

Some psychoanalytic theories have shown that all humans have natural drives and urges that are repressed in the unconscious which suggest that humans have inherent tendencies towards wrongdoings. Reasons behind people committing crimes are obviously many, varied and sometimes complex.

Fundamentally, **routine activity theory (RAT)** states that when three elements of opportunity, motivated offender and absence of capable guardian coincide in time and space as conditions for a crime to occur. Crime perpetrator could be internal or/and external.

- **Opportunity is the most influential:** This is a

particular concern for business since assets need to be easily accessible to staff, and sometimes customers.

- **Motivation is also crucially important:** Most people when presented with the opportunity do not commit acts of dishonesty. Motivation may take the form of carrying out an act of violence to impress others, rationalization, temptation, accessibility and reward.
- **Availability of Means or Absence** of a capable guardian refers not only to security measures, but also to poor design of the environment in failing to create natural surveillance and territorial ownership.

**There are two major ways to prevent crime;**

1. Change people's criminal motivations
2. Reduce opportunities for crime

General Crime prevention is the anticipation, recognition, and appraisal of a crime risk and the initiation of some action to remove or reduce it.



*Key information*

*Crime prevention is a pattern of attitudes and behaviors directed at reducing the threat of crime and enhancing the sense of security, to positively influence the quality of life in our society, and to develop environments where crime cannot flourish.*

*—(National Crime Prevention Council, 1990).*

The primary objective of an efficient security structure is the **PREVENTION OF CRIME** but it has been overshadowed by growing emphasis on protection system. As such, target hardening is now seen as a system of prevention where individuals must actually use devices for effective crime prevention, such as locks, door systems, lights, alarms, etc.

Crime prevention is a proactive security practice and it is being underpinned by seven (7) principles.

**Preventing crime is;**

1. Everyone's business
2. More than just protection
3. Linked with solving social problems
4. Cost-effective
5. Education
6. Tailored to local needs and conditions
7. Continual testing and improvement

**Benefits of Crime Prevention**

- A revived sense of personal civic responsibility
- Greater freedom and security
- Increased respect
- Increased individual and collective pride in self and community
- Healthier, more interdependency
- It saves money

*Key information*

*A successful security strategy concentrates on understanding the motive, limiting the opportunity and obstructing the means proactively.*

## Crime Prevention Strategies

A very straightforward taxonomy of crime prevention strategies is to classify measures as primary, secondary and tertiary.

Primary measures focus on treating the conditions specific to the offence, while secondary and tertiary turn their attention to the offender.

**A. Primary Prevention:** Effecting conditions of the physical and social environment that provide opportunities for or precipitate criminal acts. It is a combination of Crime Prevention through Environmental Design (CPTED) and Situational Crime Prevention (SCP).

### Core elements of CPTED

1. Provide clear border definition of controlled space.
2. Provide clearly marked transitional zones.
3. Relocation of gathering areas.
4. Place safe activities in unsafe locations.
5. Place unsafe activities in safe locations.

6. Redesignate the use of space to provide natural barriers.
7. Improve the scheduling of space.
8. Redesignate or revamp space to increase the perception of natural surveillance.
9. Overcome distance and isolation.

## Core elements of SCP



- B. Secondary Prevention:** It is being engaged in early identification of potential offenders and sought to intervene before the commission of illegal activity. Organizations execute Secondary Crime Prevention in a variety of ways such as employee screening, awareness training and socialization.



**C. Tertiary Prevention:** Dealing with actual offenders and intervention. It is about punishment and sending clear signals to wrongdoers or potential wrongdoers.

*There are four key areas that require expertise focus when developing a crime prevention programme that will be applicable to crimes perpetrated both externally and internally;*

1. **Procedural Security:** It is always important to maintain incident databases, collect crime data from different sources and analyse them for intelligence derivation. Ensure to conduct security risk analysis, develop and implement strategic security plan for sustainable security culture. Building a healthy security culture helps to reduce or prevent crimes because in continuous influence the offender's decision or ability to commit crimes.
2. **Motivation to Dishonesty:** Creation of an atmosphere of zero tolerance toward crime and criminal activity. This is closely linked to procedural security; this includes activities such as background screening, security awareness training, and employee socialization.
3. **Environmental Design:** Prevent crime through designing a physical environment that positively influences human behavior by designing out opportunities and designing in natural

surveillance.

4. **Physical Security:** It goes without saying that the application of physical security measures (access management, guarding, intrusion detection, surveillance, lighting, barriers and fencing, locks, strong doors and windows, contraband detection etc) will minimize crime opportunities and accessibility to targets.

In today's security management, it is smart to focus on crime prevention as a foundational strategy.



*Key information*

*Active and successful crime prevention programs not only reduce crime and save lives, but they provide peace of mind.*

*It is important to be aware that crime can occur anywhere at any time.*

## 10 Principles of Crime Prevention



1. **Target Hardening:** Making asset difficult for an offender to access.
  - Upgrading the locks on your doors, windows, sheds and outbuildings.
  - Using secure passwords on online accounts to prevent criminals hacking.



2. **Target Removal:** Ensuring that a potential target is out of view
- Not leaving valuable items on view through your windows.
  - Being cautious about what you post online.



3. **Reducing the Means:** Removing items that may help commit an offence
- Good housekeeping: Not leaving tools and ladders that may be climbing aid or damage.



4. **Reducing the Payoff:** Reducing the profit the criminal can make from the offence.
- Security marking your property.
  - Not buying property you believe or suspect to be stolen.



5. **Access Control:** Looking at measures that will control access to a location, a person or object.
- Regulating movements IN & OUT of a building or facility.
  - Ensuring that fencing, hedges, walls and other boundary means are active.



6. **Surveillance:** Improving surveillance around homes, businesses or public places to deter criminals.

- Removing high hedges/shrubs that may affect line of sight.
- Consider adding CCTV to a commercial site or public place
- Establishing a human watch



7. **Environmental Change:** Ensuring your property and wider community looks cared for.

- Working with the police and local authority to close a footpath
- Ensuring that graffiti and domestic/commercial waste is cleared up



8. **Rule Setting:** Changing our habits by setting rules and positioning signage in appropriate locations.

- Introducing a rule that regulates ingress and egress of persons/items.



9. **Increase the Chances of Being Caught:** Increasing the likelihood that an offender will be caught to prevent crime occurring.

- Making use of dusk to dawn

security lighting is actively in place.

- Using professionally configured CCTV and/or alarm systems.
- Upgrading security to delay an offender.



**10. Deflecting Offenders:** Deterring an offender or deflecting their intention.

- Using automated or telemetry systems to make homes/offices look occupied if vacant after the hours of darkness.

# SECURITY AS ASSET PROTECTION



**T**his security approach seeks to control, defend or eliminate a manifest threat. It is a condition of being protected against threats/hazards, loss or risks. **Protection** could be simply defined as the concept of **SAFEGUARDING** and strategies for **Risk Management**.

**Key information**

*Usually, asset is vulnerable due to its usefulness or value but not utilized if the vulnerability cannot be exploited when effectively (through risk management) safeguarded.*

A safeguard is simply an element or component of the protection system.

Protection system integrates people, procedures, and equipment for the security of assets against threat.

The origins of security systems are obscure, but techniques for protecting the household, such as the use of locks and barred windows, are very ancient. As civilizations developed and developing, integrated security systems (*passive and active measures*) referred to as **Protection System** in this case becomes very necessary.

Most security and protection systems emphasize certain threats/hazards more than others. In a retail store, for example, the principal security concerns are shoplifting and employee dishonesty (e.g. pilferage, embezzlement, and fraud).

There are three primary categories (**core elements**) of security as asset protection. These include management security, operational security and physical security.

**Management Security:** It is overall design of security architecture which provides the required guidance, policies, and procedures for implementing a security environment. It is a strategic approach to protection of assets and this is different from Security Management.



**Operational Security (OPSEC):** It is also known as procedural security, is a risk management process that ensures functionality and compliance of all the security architecture elements. It is a tactical approach to protection of assets. OPSEC process requires the following three key steps;

1. Identify your assets (critical and non-critical)
2. Characterize the assets
  - Identify possible threats
  - Assess the existing safeguarding measures
  - Analyze all related vulnerabilities
  - Appraise the level of risk associated with each vulnerability
3. Put countermeasures in place



## **OPSEC Best Practices**

Follow these best practices to implement a robust, comprehensive, operational security program;

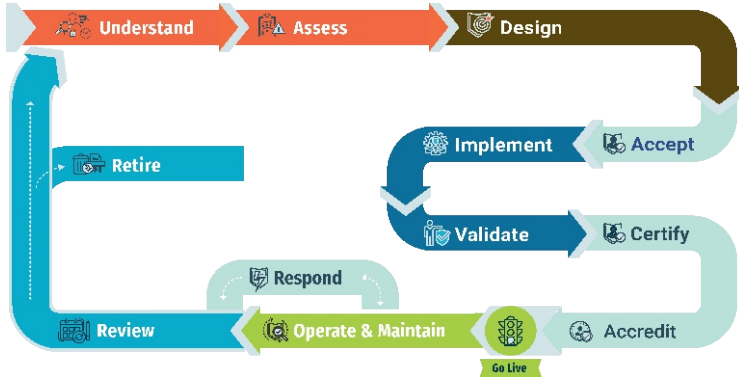
- Implement precise change management processes
- Automate task to reduce the need for human intervention
- Incident response and disaster recovery planning
- Evaluate and review performance

## Physical Security

Physical security is pretty much exactly what it sounds like. It is the system used to secure physical space and assets. This system encompasses technologies, processes and professional personnel for assets protection. Gone are the days when an organization and its assets could be protected by merely employing a few security guards, it now requires system integration.

### Physical Security Lifecycle

Understanding the physical security lifecycle will enable you to establish and maintain robust asset protection systems.



Designing principles that underpin physical security systems (**PSS**) are;

- a. **Deter:** Dissuading adversaries from conducting an attack by emphasizing the likelihood of failure and capture.

- b. **Detect:** Initiating an appropriate response to a threat or attack as early in the attack timeline as possible.
- c. **Delay:** Implementing measures to slow the progress of harmful event as long as possible to allow an effective response deployment.
- d. **Respond:** Preparing measures to prevent, resist or mitigate the impact of an attack or event.
  - a. **Recover:** Recovery is your plan to continue business and operations as normally as possible following an incident.
  - b. **Re-evaluate:** This is very critical. You must constantly keep your PSS under review and keep re-visiting the initial assessment and objectives so as to ascertain any change or new threats for possible mitigation adjustments.

Each of these elements has to be planned in relationship to the others.

- *It may not be necessary in spending money on expensive perimeter fences if there is no detection system in place to warn of intrusion.*
- *Installing sophisticated detection systems if there is nobody around to respond to any triggered alarm is inadequate.*
- *And there is little point in having deterrence and detection without delay if an intruder can gain access, cause damage and get away because there*

*were no delaying measures in place or response times were too slow.*

- *Extreme security countermeasures should not be implemented if they disrupt operations or adversely affect the safety of the occupants of a building.*

## Designing Comprehensive Physical Security

At the planning stage, there are two scenarios: IF and WHEN to be duly considered.

- The “*if*” scenario covers planning and procedures to prevent the likelihood of an incident.
- The “*when*” scenario covers planning and procedures after an incident and is mainly concerned with mitigation and recovery



### *Key information*

*Remember that the cost to mitigate and recover may be less than the cost to protect, so there always has to be a balance between protection and mitigation.*

## Design Process

This design methodology walks you through the five steps needed to identify critical assets, identify threats and targets and take the appropriate mitigating

measures to implement an effective integrated physical security system that addresses your specific needs and requirements.

### **1st Step: Model Secure Facility**

Having been equipped with the basic security techniques and applications relating to facility protection, we next look at a model secure facility. The model secure facility is one where all critical assets have been identified, the threats to them identified and prioritized and effective security measures put in place to mitigate them.

All this has to be done in consultation with all inside and outside stakeholders with mandated requirements and all appropriate regulatory drivers. Many methodologies omit this and go straight on to the different assessment processes taken as you develop a strategic plan to implement an integrated physical security system.

However, we believe it is important that you examine what would constitute a model secure facility for you because when you come up with your model facility, you have a benchmark for comparison.

### **2nd Step: Gap Analysis**

How do you compare with the assumed Model Facility? The goal of physical security is to protect facilities, buildings and other tangible assets they contain. The most important of these assets are, of course, the people

who work in and visit the facility. The first things you need to find out are:

- The assets to be protected
- The threat to those assets
- The vulnerability of those assets
- Your priorities

### ***What Am I Protecting?***

Protective systems should always be developed for specific assets. You have to know the core functions of your facility because that will enable you to identify the specific critical infrastructure that you need to protect to continue in business in the event of an attack.

### ***Who Are My Adversaries?***

It is important to identify and characterize the threats to these assets. These threats can come from within or outside the building.

- Internal threats include pilfering of office equipment or theft of classified information. Internal threats also include disgruntled employees who may sabotage equipment or attack other employees.
- External threats range from vandalism and break-ins to acts of terrorism.

You need to know your adversaries and the various tactics they might use as well as their motivations and capabilities using the following tools:

- **Design Base Threat (DBT)** analysis to help identify your likely adversaries, their strengths and capabilities, what their targets might be and the likelihood of them attacking you and, if so, how.
- **Crime Prevention Through Environmental Design (CPTED)** to take into account the relationship between the physical environment and the users of that environment. It is one of the tried and trusted methodologies available to you and is a useful tool in identifying the “*bad boys*” and what crimes may affect your facility and personnel.

### *Where Am I Vulnerable?*

Until you discover your areas of vulnerability, you cannot develop the strategies needed to protect them. A useful way of identifying threats is to conduct scenario-based assessments. This is very crucial analytical process because you must be able to identify all critical flaws and weak points in your current physical protection. You have to come up with multiple “*what if*” scenarios and work them through. By working through the various scenarios and determining the probable actions and consequences, you can then develop plans to counter or mitigate them. Use the model facility as your benchmark to identify the areas that need attention. Conduct an audit of the facility – site boundaries, building construction, room locations,

access points, operating conditions (working hours, off-hours and so on), existing physical protection features, safety considerations and the types and numbers of employees and visitors.

Next, determine all critical assets – tangible and intangible, equipment, personnel and materials. This analysis should also include reputation, morale and proprietary information. You must identify and characterize vulnerabilities – weaknesses – that would allow identified threats to be realized. By identifying your weaknesses you are able to develop solutions to eliminate them.

### *What Are My Priorities?*

Risk assessment must take into account the effect on business or operation if assets are destroyed or damaged. Part of that assessment is to rate the impact of the loss of those assets on a scale of low, medium or high. This will identify the critical assets that need maximum protection.

### *How Do I Now Compare?*

Once you have established answers to the above questions, you are in a position to do your Gap Analysis to identify what needs to be done to reduce risk, increase safety and provide the necessary physical security for your building and people.



### **3rd Step: Gap Closure**

Having identified all the relevant shortfalls, you must then consider and evaluate all available options to mitigate the threats. There is a vast array of external and internal systems and devices available. You must determine which are the best options and combinations for your particular circumstances. If you have questions, consult an independent physical security consultant rather than a vendor with a vested interest in selling you just his/her products.

Security technology includes, but it is not limited to;

- Closed-circuit television –CCTV
- Intruder Detection/Prevention Alarm Systems
- Access Control
- Telemetry or Global Positioning Systems
- Electronic Locks
- Weapon Detection Equipment
- Emergency Alarm and Evacuation System

### **4th Step: Strategic Plan**

Having identified assets, adversaries, threats, vulnerabilities and determined priorities and options, you are now in a position to plan and strategize the security change process. This means developing a road map – you know where you are and have to plot how you are going to get where you need to be. The strategic plan serves two critical functions: It is the marketing tool you need to get management approval and it is the blueprint for your physical security plan.

The strategic plan sets out Steps Two and Three state above by documenting the gap analysis, identifying critical assets, threats and weaknesses and all areas needing to be addressed. The gap closure documents how you plan to close those gaps, the justification for the actions to be taken, costs involved and time frame for implementation.

### **5th Step: Implementation**

Once your strategic plan has been approved, it must be implemented. This includes project management, bid contracting and vendor selection, quality assurance and quality control, and revising policy procedures. Integrated physical security planning is also an ongoing requirement. Once your system is in place you must continuously test it for weaknesses and vulnerabilities. You must ensure your employees understand the measures in place and what they must do in the event of an emergency. Re-analyze your current situation. Ask yourself what has changed and what new threats have emerged. By constantly tracking and monitoring your integrated physical security system you can close any gaps and introduce enhancements.

Above all, the physical security plan must be implemented with the management and employee buy-in, to budget and on time with minimum ongoing disruption to the facility's day-to-day operating procedures

*You will learn about the implementation later in Section Five.*

## Rule of thumb

Throughout this process you must ensure:

1. **Confidentiality** – the need to protect critical planning documents
2. **Appropriate Public Relations** – keeping the right people in the know while ensuring that information did not get into the wrong hands
3. **Sustainability** – incorporating existing systems into the plan rather than replacing, implementing baseline security where appropriate, balancing physical protection systems with operational procedures Compliance with all industrial guidelines and legal and regulatory requirements
4. Constant review and revision to accommodate new circumstances or threats.



### Key information

*Summarily, security as asset protection system is any of various means or devices designed to guard persons and property (assets) against a broad range of security threats and safety hazards.*

# SECURITY AS RESILIENCE



**I**n today's globally connected business environment, with its range and complexity of risk, requires a sophisticated approach to developing a strategic security management system, to give enterprise leaders the confidence that their business is as resilient as it can be to these risks.

Resilience is a much abused and maligned term. It is most logical when used ordinarily, but it has come to mean anything from an enterprise's rapid adaptability to change, through to having business continuity and

emergency management plans in place.

*Hence;*  
*Resilience = Business Continuity Plan*  
*+ Emergency Management Plan*

It is about;

- Surviving inevitable attacks and penetrations
- Continuing to do business even under attack
- Discovering breaches and containing them
- Ultimately prevailing in spite of them
- Being prepared for the unexpected



*Key information*

*Simply put, it is a behaviour, an ability or/and principle.*

Whenever threats cannot be controlled, eliminated, security as resilience focuses on the ability of social systems to “**bounce back**” and recover from shocks due to insecurity. It is also a capacity of security architecture to respond to a perturbation or disturbance by resisting damage and recovering quickly.



*Key information*

*Business resilience management is critical to business survival in the face of rapidly changing security threats and regulatory environments.*

*“It is not the strongest of the species that survives, or the most intelligent that survives. It is the one that is most adaptable to change”* –Charles Darwin

**Business Continuity Institute (BCI)** defines organisational resilience as *“holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities”*.

It is the ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruption in order to survive and prosper.

Detailed risk and resilience assessments help to identify gaps in security strategy and present recommendations on measures to minimize or mitigate those risks in future.

The key five attributes (5-Ps) of a resilient organization

1. **Prepare:** Create a robust and an integrated risk framework.
2. **Prevent:** Coordinate responsibilities across Enterprise Risk Management and Business Lines.
3. **Protect:** Understand operational risk at various levels – frequency, severity, and velocity of risks to develop appropriate controls and mitigation.

4. **Practice:** Implement crisis management best practices to effectively respond to risk.
5. **Pivot:** Monitor the effectiveness

Business resilience is an enterprise-wide term which encompasses crisis management and business continuity, and responds to all types of risk that an organisation or a team may face.

- **Business resilience** is more a **strategic risk management approach**, which integrates many disciplines into a single set of integrated processes, and is tailored to an individual organisation's requirements.
- **Business continuity** is a process-driven approach which can be standardised, and which leads an organisation out of a major incident so that it can continue operations.
- **Crisis management** addresses specific crises (man-made and natural events).

## Resilience Development Strategy

In order to ensure the resilience of an organisation in the face of these varied risks, it is essential to have a business resilience strategy, which should have five core strands:

1. Understand and analyse market trends, threats and risks
2. Assess and consider potential opportunities to exploit

3. Develop adaptive leadership framework
4. The development of a learning culture
5. Double loop learning methodology

### **Top Threats to Business Continuity Plan –BCP**

- **Global Pandemics**
- **Natural Disasters:** Weather related such as tornadoes, hurricanes, tsunamis, etc.
- **Utility Outages:** Loss of power generation
- **Cybersecurity**
- **Sabotage**

### **Four (4) Characteristics Guiding Business Continuity Planning**

1. **Comprehensive:** You may never be able to plan for every single possible disruption – or the combinations thereof – but it is worth trying.
2. **Realistic:** Ensuring to have many contingency plans built in.
3. **Efficient:** Business is complex, so you won't sit there and say your business continuity plan needs to be simple but it needs to be able to run efficiently with available resources.
4. **Adaptable:** Nothing on paper could ever compare to the curveballs that nature or other unexpected forces may throw at us. Leave lots of room in your plan to adapt to the moment, as circumstances change – sometimes minute to minute.



---

## Creating Business Continuity Plan

Creating a business continuity plan is, admittedly, probably not the most fun day you'll have at work but it is a critical piece of running a resilient business. It's important that you, your business continuity team, and the rest of your staff take this seriously.

1. **Identify objectives and goals of the plan:** The highest level, the objective of creating a business continuity plan is to keep essential business processes running or minimize disruption. But every business is different — so you'll need to identify the goals and objectives most important to the way you operate. Those goals will guide your risk assessment, the business continuity planning process, and potential recovery strategies.
2. **Establish an emergency preparedness team:** Select a few cross-functional managers or leaders, and anyone else you identify who may bring something valuable to the table. Ensure that someone is designated as the leader to keep things moving forward and make decisions when necessary.
3. **Perform a risk assessment and business impact analysis (BIA):** Here's where you'll identify the biggest potential threats to your business, then research and analyze them thoroughly. Discuss with the team what would happen if you have to reduce, modify, or eliminate essential services or

functions. Be sure to document all the identified issues and related business impact.

- 4. Identify essential services/functions business functions:** You will have to determine how your organization will maintain essential services/functions in the event of an emergency



*Key information*

*Summarily, business continuity and resilience encompasses planning and preparation to ensure that a business can continue to operate in the event of a critical incident or disaster and can recover to an operational state within a reasonable period.*

If something can go wrong, it probably will. And the time to repair roof is when the sun is shining and the future belongs to those who prepare for it now.

Go beyond traditional physical security management to build an enterprise-wide risk and resilience-based security.

*Nothing is ever certain.*

Section

# 4

## PHYSICAL SECURITY TECHNOLOGY



*This section addresses the main categories of physical security mechanisms, to include deterrent, detective and preventive measures, and explain how they might be put in place to mitigate physical security issues.*

*Effective physical security of an asset is achieved by multi-layering the different measures – known as 'defence-in-depth'.*



# PHYSICAL SECURITY SYSTEM

## *Overview*



**P**hysical security system (**technological solutions**) has traditionally been viewed as an unattractive and tedious topic that few want to tackle; however, it is important to know that safety and security must be adequately addressed. Physical security is – or should be – at the core of any business operation.

Is the prospect of implementing physical security system at your workplace or organisation intimidating?

Are you concerned that good physical security system relies on expensive secrets protected by industry experts?

Well, I am here to tell you that it doesn't have to be that way.

With cutting-edge technology and the Internet of Things (IoT) revolution, the world of physical security has drastically changed – ensuring fit-for-purpose physical security system has never been easier. Every business is capable of developing a world-class physical security program. This short guide presents everything you need to plan, design, implement, and test your physical security program.

This book contains everything you need to plan, design, implement, and test your physical security program

**Physical Security System:** It consists of the tools (hardware), people, and protocols that an organization uses to:

- Ensure the day-to-day safety of employees and business resources
- Control access to business or personal assets
- Deter potential threats
- Detect active threats
- Respond to threats
- Protect against day-to-day risks

However, as threats evolve and as bad actors become



more intelligent, and with the goal of being both proactive and reactive – the need for a robust, comprehensive physical security strategy is paramount.

Physical security is the final frontier as well as the last line of defense. When our everyday objects are susceptible to breach, it is imperative to ensure something stands in the way of us and them. The first line of physical security for your property is the perimeter, more specifically, the points of access.

The gates may be beautiful, but they also serve a security purpose. Physical security system need not be gold plated, basic security options such as automated gates are a great place to start and which may include other features and accessories, including but not limited to cameras, digital keys and voice communications between the occupants and whoever stands at the gate.

### **Essential Components of Physical Security System**

Physical security system can be divided into four distinct operations, with technical solutions available to support each:

1. Access Control
2. Surveillance
3. Deterrence
4. Response

These operations need to work together (unified solution) as part of an overall program for effective

protection. A unified solution is developed from square one to not only work together but to purposefully intertwine functionality to offer a powerful user experience that includes built-in reporting and alarm management functionalities.

With unification, it's possible to configure and manage video cameras, access-controlled doors, print badges, monitor intrusion panels and have everything at the security officer's disposal to ensure a high level of functionality from within a single platform (software/hardware).

Unification is about much more than just security.

## **Physical Security System Implementation**

Right now, you probably have just one particular physical security problem that you want to solve. Let's go through the process you should follow to design and implement the best system for your needs. The design of effective physical security system requires a methodological approach.

An effective physical security system integrates people, procedures, and technology for protection of the assets against thefts, sabotage, and malicious human attacks. Hence, the designer or security manager should weigh the objectives of the physical security system clearly against available resources and then evaluate the proposed design to ascertain how well it meets the



objectives of the security program.

To start with, a comprehensive security risk assessment is essential prior to design the effective physical security system. The PSS (Physical Security System) might waste valuable capital on unnecessary protection or fail to provide sufficient protection at critical points of the facility if comprehensive security risk assessment is not carried out.

Another important thing to keep in mind is a performance based system design is always effective than compliance or features based system. Because performance-based system design provides clear performance measures that can be validated with numeric characteristic for various system components.

This performance-based system is also quite helpful to build the business case to persuade the business leaders to by highlighting clear cost benefit analysis.

### **Risk Assessment and System Design Methodology**

An effective PSS design should have a process that produces the design as per DBT (Design Basis Threat) and not on mere assumptions or experience of the individual designing the system.

1. Plan or determine PSS objectives
2. Design or characterization of PSS
3. Analysis and Evaluation of PSS
4. Implement PSS

## A. Plan

To get the most value from a physical security purchase, you need to define your desired objectives;

- Improved safety
- Better compliance
- Alignment of security operations with strategic goals

In order to develop the objectives, the designer must accomplish three steps. Those are Facility Characterization, Threat Definition, and Target Identification.

- **Facility Characterization**

In this step, you need to understand the facility itself by assessing the facility's operations, conditions, operating states and the entire layout of the facility such as site boundary, building location, building interiors floor plans, access points, blueprints, process descriptions, health, safety and environmental analysis reports etc. Additional considerations are for any operational, safety, legal liability or regulatory requirements while designing PSS.

- **Threat Definition**

The second step in determining the objectives is to define the threat by collecting information about the adversary's Class, Tactics, and Capabilities.

**Classes of adversary:** An adversary can be categorized into three classes – outsiders, insiders and outsiders working in collusion with insiders.

**Tactics of adversary:** Deceit, stealth, force, or any of the combination is the range of tactics each class of adversary can use to defeat PSS. For instance, Deceit is an attempt to defeat a security system by using false authorization or identification. Stealth is an attempt to defeat a security system by using covert means. (Spoofing or bypassing a sensor). Force is an overt, forcible attempt to overcome a security system,

**Capabilities of adversary:** Identification of the most likely threats and system should be designed to meet those threats by the keeping their capabilities in consideration.

- **Target Identification**

The final step is to perform target identification for the facility. A thorough review of the facility and its assets should be conducted. This may include identifying critical assets, people, information or critical equipment or processes or reputation anything that could impact business operations. For instance, determining the negative impact or unacceptable consequence in the event of loss of an asset or sabotage of an equipment or interruption of a business process will help identify critical assets, or equipment, or process that needs to be protected.

Other determinant factors are;

1. **Identify Stakeholders:** Stakeholders are the people inside (internal) and outside (external) your organization or homes who care about how your new physical security system will operate.
2. **Understand Their Expectations:** Seek input from your stakeholders about what outcomes they want to see from the new system installation. Do they have any particular concerns about how it will be installed and used?
3. **Determine How to Assess Performance:** What key indicators will determine how effectively your new system does its job? For example, if you're considering purchasing a key control system, you might want to track the number of lost keys reported in your business to see if that number goes down. Or you might decide to use the number of rekeying your business has to do each quarter as a measure of security breaches.

## **B. Design**

Once you agree upon the outcomes or objectives you're hoping to achieve and how you're going to measure performance, you can get down to designing your new physical security system.

- **Ascertain required functionalities**

The primary functions of a physical Security

system are;

1. Detection of an adversary
2. Delay of that adversary
3. Response by security personnel (Guard Force)

Integration of PSS components (people, procedures, and technology) with PSS functions (detect, delay and response) produce better PSS objectives.

The integration process includes better combining the elements such as barriers, intrusion detection systems, access control systems, video surveillance, communication devices, procedures, and security personnel into a physical security system that can achieve the protection objectives.

An effective PSS should meet protection objectives within the operational, safety, legal and economic constraints of the facility.

- **Identify Necessary Products**

The design phase is the correct time to purchase any tools or integrated security systems that you will need. You already understand the outcomes you hope to achieve, so you can evaluate each product against those needs to see how well it might perform.

If your goal is to protect and track physical keys, consider exploring a key management system. If

you'd like to secure or track physical assets or people, consider secure storage and real time location and tracking products.

- **Plan Installation Location**

Now you need to decide how your new system will fit into the day-to-day workflows at your organization. Think about when and where staff will need to use it. Will your new system need to integrate with other existing security products or building infrastructure?

- **Determine System Configuration**

If the physical security systems you've purchased can be customized, now is the time to do that. Also, determine what physical layout you want your system to have. Will any of the integrations you've identified require software updates?

If your new system uses access control, decide which access control method you will deploy. This method could be one you already use at your organization or something separate.

If you want to choose a separate method, some options could include PIN codes, proximity (proximity) cards, mobile phone apps, RFID tags, or biometrics like iris scans or fingerprints. We'll go over access control in more detail in the next chapter.

## **C. Analyse and Evaluate**

Once the PSS is designed, it must be analyzed and evaluated to ensure that it is meeting the physical security objectives. To estimate the minimum performance levels achieved by a physical security system more sophisticated qualitative and quantitative analysis techniques can be used.

Generally, quantitative analysis will be used in systems that are designed to protect high-value critical assets and qualitative techniques used in systems that are designed to protecting lower value assets. In order to complete a quantitative analysis, performance data must be available for the system components.

The outcome of this analysis process is a system vulnerability assessment which will find that the design effectively achieved the protection objectives or it will identify weaknesses.

If the protection objectives are achieved, then the design and analysis process completed but If the PPS is found to be ineffective, the designer needs to redesign or upgrade the initial protection system design to correct the identified vulnerabilities.

Then, an analysis of the redesigned system is performed. This cycle continues until the outcome indicates the PSS meets the protection objectives.

## **D. Implement**

### **Installation**

Correctly implementing a new physical security system requires more work than just setting up some hardware and software. An experienced system installer or integrator is required.

### **Commissioning**

There is need to define appropriate policies governing the system's use.

- Who will use it?
- How will it be monitored?

### **Training**

Also, there is need to train employees on how to use the system effectively and efficiently. Probably one of the most complicated and unpredictable components of business security is managing the human element. In business security, people are both an asset and a liability.



## Access Control System

Access Control solutions manage the flow of traffic through facility entryways and access points. Access Control solutions manage the flow of traffic through facility entryways and access points.



### Key information

*Access control is defined as the process of selectively restricting and managing the ability to enter or exit a specific area.*

Access control systems have evolved over the years as business with increase in security. Rather than relying on mechanical keys, security guards, and paper sign-in sheets, electronic access control systems use computers and advanced technology to improve control and monitoring.

They can be used to restrict access for different types of persons: employees and visitors. Although security guards and other personnel can perform access control when needed, in most cases, it is more cost-effective to use a technical access control solution.

### **Those technical solutions can include:**

#### **1. Electronic Access Control**

Electronic access control limits access to an area, equipment, or information based on an electronic

credential and/or code. The credential or code is presented to a reader or keypad that sends information to a control unit where access privileges are stored. The control unit makes a grant or denies access decision based on its programming.

## 2. Control Unit Type

- **Standalone Control Unit:** It is a single door system and does not share data with any other control units
- **Networked Control Unit:** It is a multiple door system with ability to communicate with other control units via a network.



Electronic authentication can be achieved using a token system, such as:

**Swipe Cards:** Identification data is stored on a

magnetic strip, like on a credit card. The card is swiped at a reader to authenticate the holder.

**RFID Fobs:** Radio frequency identification keychain tokens that communicate over short-range wireless. The fob is waved near a reader to authenticate.

**Proximity Cards:** Flat cards that are pressed against readers to authenticate the holder. Newer proximity cards use embedded RFID antennas to transmit credentials.

**Mobile Phone Apps:** A secure app on a user's phone identifies them when they approach access points. Phones authenticate the holder by transmitting their identity over Bluetooth or NFC, short-range wireless antennas common in mobile devices.

## Card Readers & Credentials

Readers are devices that are used to electronically “*read*” a credential. When a credential is presented to the reader it sends the credential's information to the control panel or networked system hub to determine if access should be granted. If granted, the reader will send an output signal to release a door locking mechanism.

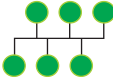

Readers are often equipped to recognize the most common form of credentials including cards, key fobs, and smartphones. There are also readers that work with a keypad for passwords or even more advanced readers using biometric scanners and facial recognition.

## Card Reader Technologies

**Card readers differ in two important respects:** Scan frequency and protocol.

- **Scan Frequency:** 125kHz vs. 13.56MHz The most common scan frequencies for readers are 125kHz and 13.56 MHz. 125kHz is proven technology prevalent in the USA and in Eastern Europe. The cards and readers tend to be lower priced. 13.56 MHz is newer, more secure technology prevalent in EMEA and increasingly in APAC countries. Hardware is currently priced somewhat higher.
- **Protocol:** RS-485 vs Wiegand Decide early

whether to use Wiegand or RS-485 technology for the readers; each has its own advantages and disadvantages as shown in below table;

	RS-485	Wiegand
Wiring Topology	Bus (Chain) 	Star 
Maximum Cable Length	1200m	100m
Number of wires needed for the Reader	4	10

## Credentials Technology

Decide on the credentials technology you wish to use. For Wiegand readers the choice includes e.g. iCLASS (3.56MHz) and EM (125kHz) cards. For RS-485 readers there is a wide choice: MIFARE, HITEC or LEGIC.

## Card and Reader Compatibility

Care must be taken when purchasing cards and readers to make sure the units are compatible. The generally accepted generic industry is 26 bit format. Many vendors offer proprietary data formats (from 21 bits to 40 bits) designed to work only with their systems, but most of these systems can also accept 26 bit formats cards.

## **Touchless Access Control**

Covid-19 pandemic has recently caused a shift in preferences for access control security. People no longer want to touch public door handles, push buttons on elevators, or swipe a proximity card reader for an access control system for fear of infection. Instead, they prefer touchless, contactless and hands-free control of door access. Touchless Access Control is designed to offer a contactless way for the employees and visitors to enter the commercial or communal building. With touchless access control systems, you can eliminate any need for physical contact. Employees can use face recognition, hand wave gesture, or mobile apps to get inside the building without ever having to touch a keypad or door

## **Locks**

Lock selection is a critical part of access control system design. There are several common types of locksets;

- Electric Strike
- Magnetic Lock (Maglocks)

## **Door Security**

Door/lock status monitoring is an essential part of the complete security of an access control system. Maglocks and strikes provide security above conventional mechanical hardware, but neither product is foolproof. The simplest way to monitor door is using a door contact.

## Access Control Software

Access control software is used to manage the system and to allow for authentication, authorization, access, management, auditing, and reporting. Systems can range from small set-ups with a few doors to multi-location enterprises with thousands of doors. Additional features allow for remote management, monitoring security cameras, sending mass notifications, lockdowns in emergencies, and more.

### Important Programming Features

- **Access Group:** It is a set of time zones and a group of doors which are associated with a group of system users.
- **Anti-Passback:** It is a method which helps to facilitate greater security for entry and exit so as to prevent tailgating.
- **Automatic Lock/Unlock:** Automated way of locking or unlocking specific door at a programmed time.
- **Door Held Open Output:** If a door is held open for an extended period, an output (alarm) can be activated.
- **Forced Door Output:** If a door is forced open without presentation of a valid user card or credential, the access control system can activate an output (alarm).
- **Holiday:** This allows the system to override time zone and door permissions to restrict

access during holiday hours.

- **Input:** Most access control panels have ability to monitor external devices through inputs which could be used for monitoring purposes.
- **Relay Output:** It is used for controlling lock hardware or other devices/systems (telemetry).

Electronic access control systems are very secure, but they can be expensive if properly deployed. Most organizations only deploy electronic access control at their most sensitive access points.

- **Mechanical Access Control**

Given the high cost of electronic access control, most doors and other access points continue to be secured using mechanical lock-and-key systems. Mechanical access control is cost-effective for managing access points with routine levels of security.

The major downside to using mechanical controls is that they lack built-in tracking and accountability. Because electronic systems communicate with a central computer system for every access request, they generate a complete access log in real time. Mechanical keys don't have this in-built capability.

- **Key Management Systems**

They are secure cabinets with electronic



access control terminals attached or configured. Combining mechanical access controls with an electronic key management system is one model that most organizations employ as a cost-effective alternative to electronic access control.

Users authenticate themselves at the terminal and specify which key ring they want to sign out. The request is logged, and the key management system unlocks only the selected key-ring.

Key management systems are time consuming administrative tasks but can be automated. Take for instance, managers can set curfews on key sign-outs or limit the number of keys a single employee can have in their possession. If an employee misses a curfew or does not return their keys at the end of their shift, the key management system can send alerts to the employee's supervisor.

- **Asset Management Systems**

As with keys, many businesses find it beneficial to control access to sensitive or expensive asset. Like key management systems, asset management systems use a combination of secure cabinets, access control terminals, and smart sensor

technology to control who uses assets, as well as when and how assets are used.

Content surveillance sensors inside locker compartments can identify assets when they're signed out or returned for better accountability and inventory tracking.

## Surveillance System

Surveillance is the process of gathering information relevant to an organization's physical security. The gathered information commonly includes the locations of potential threats, persons, and valuable equipment moving through your facility, as well as the activities of security personnel.



*Key information*

*Security surveillance, the act of monitoring a certain activity, place, or person for safety reasons, is a growing market.*

Security surveillance system used to prevent crime in private and public locations.

## Video Surveillance

Video surveillance systems are more important than ever in today's business environment. All businesses – large or small – need an effective system to protect their

assets and remain profitable.

## Why Businesses Need Video Surveillance

Investing in a video surveillance system affords organisations or business owners several benefits. When installed inside and outside the workplace, they help detect vandalism, criminal activity, or any other improper behavior for investigation purposes.

This includes employee theft, which is more common than most business owners assume. According to the Association of Certified Fraud Examiners (ACFE), a business is probably losing more than 5% of the annual revenue to employee theft. Small businesses (less than 150 employees) are at the highest risk – accounting for 80% of employees theft.

Also, it helps boost businesses' bottom line by encouraging employee productivity and helping in the detection of faulty equipment. Along with ensuring regulatory compliance, they foster a sense of security and peace of mind.



Video surveillance systems involve strategic placement of security cameras, monitoring motion and activity, generating alerts, transmitting footage, and storing that footage.

Cameras can be both indoors and outdoors.

The camera system may also be referred to as closed-circuit television or CCTV. The purpose of a CCTV system will typically fall into one (or more) of the following categories:

- Deterrence (Overt/Obvious)
- Observation
- Documentation

CCTV is often one of the main stays of a modern security system. Its primary focus is to act as a detection and verification system for other security measures. CCTV can be a single or combination of systems and technologies to form the overall security solution, some of these may include:

- Visible band or infrared CCTV
- Thermal imaging
- Video analytics

Security cameras can be stand-alone devices or part of a system depending upon the complexity of your security needs. In order to meet your security objectives, cameras (or signs saying cameras are present) must be visible and the cameras must be able to record, store and transmit footage (or be connected to recorder or system

that can do so).

Traditionally, video surveillance systems had to be actively monitored by security personnel to identify threats on screen. Either that or they were just used to collect footage for review if a security incident occurred.

More modern security systems use video analytics software that is capable of detecting potential threats on its own. This software can recognize cars entering a secured lot after hours, or even the motion of an attacker swinging a punch. When a potential threat is identified, the analytics system automatically notifies human security personnel so they can respond.

## Basic Concept of CCTV

A CCTV system comprises three basic elements:

- **Image Creation:** The capture device for the CCTV, usually the camera/lens combination.
- **Interconnections:** The data transmission path, which may comprise cabling, a computer or telephone network, or use of radio waves/infrared.
- **Image Processing:** Including image analysis, DVR/NVR, storage and display.

## Surveillance System Equipment

There are two types of cameras used for surveillance - analog and IP (internet protocol), which are digital cameras.

**Analog Cameras:** These are usually lower resolution than the more modern IP technology, and require cable connections to a Digital Video Recorder (DVR) to record and store footage, plus wired connections for power. To ensure the integrity of the footage, the camera must be located fairly close to the DVR and the number of ports on the DVR determines the number of cameras that can be connected. So, additional DVRs may be needed to support sites requiring many cameras. With the DVR, the footage can be viewed on a monitor in real time or a router and modem can be connected to transmit the footage.

However, the video footage tends to be grainier than digital footage and because the camera does not have digital zoom, enlarging any area of the image further reduces the clarity.

These cameras cost less than digital cameras, but because their field of vision is smaller, more cameras may be needed. There are more design options for analog cameras, so you may find the right camera for your needs at a lower cost than digital.

**Digital Cameras:** IP cameras are higher resolution, which generates clearer images but, as we said, use

more bandwidth to transmit and require more storage space.

Cameras connect to a network video recorder (NVR) via a PoE (Power over Ethernet) switch, which has ports for many cameras and then uses just one cable to connect to the NVR and power source. This reduces the number of cables needed but can put a drain on your network bandwidth.

There is no limitation to where cameras can be placed in relation to the NVR, and wireless network access enables remote viewing of footage. Also, the digital feed can be encrypted. Wi-Fi cameras do, however, raise the concern of potential hacking, so it is important to understand the security features of your cameras.

Digital cameras can have many additional features such as digital zoom, mobile notification, auto-recording triggered by motion, one-touch connection to authorities, object recognition, among others. If you are transitioning from analog to digital you may want to consider a hybrid video recorder that can support both types of cameras.

## **System Criteria**

Before you determine what cameras, recorders and storage to use, it is important to assess your security needs and budget. These will influence your system choices. Some criteria to consider as you review your needs include:

- **Number of Cameras:** Once you know the areas to cover with cameras, you can assess how many cameras you'll need. Keep in mind; analog cameras have a smaller field of vision.

*Important Note: Estimated four analog cameras to every one IP camera. So, you'll likely need more cameras if you choose analog.*

- **Indoor vs. Outdoor Cameras:** When considering the type of camera you need, keep in mind that outdoor cameras must be able to withstand the elements and are more easily tampered with than indoor cameras. This means outdoor cameras must be more durable and may have additional features to meet outdoor surveillance needs; so they can be more expensive.
- **Video Quality:** What resolution do you need for your video? High resolution is recommended as this improves the integrity of the images and may improve the chances of identifying people or evidence if a crime is committed. Frame rate is also a consideration as the more frames per minute, the better the image quality. Both of these criteria require a digital camera and also increase your need for storage space and bandwidth.
- **Storage:** The resolution of your footage, amount of footage (how many cameras are



recording), and length of time you want to store footage will dictate how much storage you will need. In addition to physical storage, there are many cloud storage options that can be used to backup your footage and also reduce the duration of time footage remains on your hard drive. You can schedule footage uploads for times when your network is not busy to lessen the impact on bandwidth.

### CCTV Storage Calculation Formula

**Storage = [(Cam\_birate/8) x 3600 x 24 x Qty\_cam x No\_days] / 1G**

- *Storage = Amount of space in GB (Gigabytes)*
- *Cam\_birate = Camera bandwidth*
- *8 = To convert from bits to bytes*
- *3600 = To convert from seconds to hour*
- *24 = To convert from hour to day*
- *No\_days = Total number of days*
- *1G = Divide by 1G (1,000,000,000) to convert from KB to GB*

Camera Design Features. There are several camera model options including bullet, dome, pan-tilt-zoom (ptz, which allows field of vision to be adjusted remotely). You can also choose a camera that records audio or that supports 2-way audio communication. If you will need to record in dark areas, consider cameras with infrared LEDs.

- **Compatibility.** Be sure the camera(s) you select

are compatible with your recording system. While DVR is needed for analog cameras and NVR is used with IP cameras, some recorders are only compatible with specific camera brands.

- **Monitoring:** Will you have a station in your office where someone will be watching monitors? Will you want a mobile app with a feed from your cameras? Do you want to access the camera feed and footage at anytime from anywhere?
- **Legal Issues:** Surveillance systems have the potential to intrude to a significant degree on people's privacy

### Determining overall purpose of cameras

The size of the target in relation to the field of view is another key consideration when designing a system and specifying camera variables.

Purpose	Resolution pixels/FOV	Screen size
Monitor	23pixels/m	5%
Detect	35pixels/m	10%
Observe	58pixels/m	25%
Recognize	118pixels/m	50%
Identify	150pixels/m	100%

## Alarms

Whereas video surveillance systems record what is happening inside a particular location, alarm systems monitor for attempts to access to unattended sites. Different kinds of sensors are employed for different alarm functions.

Motion sensors detect movement in low light or dark environments. Perimeter sensors detect when a door or other access point is breached. Glass break sensors detect the unique frequency of glass breaking.

These are some of the most common sensor types. All of them notify security personnel to respond when a breach is detected. Burglar alarm system systems provide detection, reporting and deterrence.

**A proper design of burglar alarm system must include the following common features;**

1. Detection for all vulnerable perimeter entry points.
2. Interior detection for all expected target areas or areas of travel.
3. Security of the control panel
4. Standby power.

## Video Surveillance Integrations & Features

The world of video surveillance is changing and growing every day. Today's video surveillance features

and devices have more capabilities and intelligence than ever before. An ideal solution should streamline the processes and save on costs or time. It should integrate with other security systems (audio surveillance, access control and telemetry systems) and provide a centralized platform to ensure greater control and video surveillance monitoring.

### **Managing Video Surveillance Systems**

Video surveillance management is not limited to monitoring activities – it's a wide-reaching process. It includes;

- How you manage your security during your active and inactive hours.
- How are you ensuring your business is secure while you're gone?
- Are you equipped with the right skills and capabilities to react quickly in the event of a security incident?

With the help of remote management and cloud storage, you can stay in control of your valuable business and have peace of mind from anywhere.

## **Deterrence System**

The purpose of deterrents is to prevent threats from ever arising in the first place. They include:

### **A. Lighting**

Security lighting is the most significant crime deterrent. It enhances natural surveillance, delineates private and public spaces, can direct access and reduces fear in legitimate users. Maintaining good visibility indoors and outdoors is an excellent way to deter potential threats. Lighting is particularly important around access points, like doors and windows. It is also vital in parking lots and other areas where people are likely to be alone.

Security lighting should be installed in areas that could conceal an attacker adjacent to, as well as in, high-risk areas. Motion-activated lights help attract attention to movement making them very effective for natural surveillance. Lighting directed up and toward a facility or wall will create large shadows with exaggerated movement when an intruder passes in front, thereby gaining the attention of people from great distances.

Lighting cannot prevent disasters or attacks nor can it guarantee human safety if such unforeseen events occur. Rather, lighting is a tool that, used wisely, can increase security and safety. Used unwisely, it can waste precious resources and actually detract from these goals.

## Types of Light

- **Incandescent Lighting Systems:** have low initial cost and provide good rendition. However, incandescent lamps are relatively short in rated life (500-10,000 hours) and low in lamp efficiency when compared to other lighting sources. They are commonly used in home or in small lighting systems. The lumen per watt is 17-23.
- **Mercury Vapor Lamps:** emit a purplish-white color, caused by an electric current passing through a tube of conducting and luminous gas. This type of light is generally considered more efficient than incandescent and it is used extensively outdoors. Because mercury lamps have a long life (24,000 plus hours) and lumen maintenance characteristics, they are widely used. Good color rendition is provided and the lumen per watt is 45-63.
- **Metal Halide:** This type is similar in physical appearance to mercury vapor, but provides a light source of higher luminous efficiency and better color rendition. The rated life hours are short when compared to the 24,000 plus of mercury lamps. . Rated at 80-100 lumen per watt.
- **Fluorescent:** provides good color rendition and high lamp efficiency (67-83 LPW) as well

as long life (12,000-20,000 hours). Fluorescent lamps are temperature sensitive and low ambient temperatures decrease their efficiency. Fluorescent lights cannot project light over long distances and are not desirable flood lights. This type of light is used commonly indoors.

- **High-Pressure Sodium Vapor:** This light source was introduced in 1965 and is used for exterior lighting for parking areas, roadways, and buildings. It is also inside for commercial and industrial applications. It provides high lumen efficiency (100-140) and poor color rendition. The lamp life expectancy is up to 24,000 hours. The maintenance of this light output is good and averages about 90% throughout its rated life.

## **B. Physical Barriers**

Beyond a locked door, there are a variety of elements that can be used to prevent entry to an area. Physical barriers are often used to protect heavily trafficked or vulnerable areas. Barriers that prevent entry include: turnstiles, speed gates, security revolving doors, and interlocks. Physical access can also be used to control and protect through less conventional approaches like frosted glass and interior layout design.

Barriers are used in physical security to define

boundaries, delay or prevent access, restrict movement to a particular area, obscure visual observation into or from an area, and prevent technical penetration of an area. When barriers are selected and installed properly, they can represent not only a physical impediment but also a psychological deterrent to an attacker.

Manmade structural barriers and natural barriers are two general types of barriers.

Fences, vehicle gates, walls, even shrubbery can deter criminals looking for an easy target. A barrier that requires extra effort to cross can deter many threats from breaching your perimeter.



### *Important Notes*

1. The barriers you select and install to keep attackers out also may keep rescuers out. Work closely with



- public safety first responders to ensure they know the barriers you have used and where they have been deployed.
2. To the greatest extent possible without sacrificing security, barriers should be esthetically compatible with your facility. This is more than a “look nice” issue.
  3. Physical security measures should not attract undue attention to your facility.

### **C. Environmental Design**

Crime Prevention Through Environmental Design (CPTED) is a crime prevention theory focusing on tactical design and the effective use of the built environment, which when applied, reduces both crime and the fear of crime. The main objective of CPTED is to reduce or remove the opportunity for crime to occur in an environment, and promote positive interaction with the space by legitimate users. CPTED is basically preventive and proactive model. CPTED involves overlapping principles in the design of the built environment;

1. **Natural Access Control:** to prevent access to an area, increasing an offender's perception of detection and effort when entering.
2. **Natural Surveillance:** has the purpose of keeping potential intruders under observation by legitimate users and, again, raises the perception of intruders being seen.

3. **Territorial Reinforcement:** develops a sense of ownership and therefore control. This approach is achieved by structurally defining public and private spaces to reduce ambiguity of ownership.
4. **Quality Management:** ensures continued use of the space for its intended purpose and maintains the legitimate users feeling of safety. Proper lighting, facility maintenance, the removal of crime indicators, and vegetation management creates a perception of care.

By designing areas according to these strategies, the crime level in the built environment can be reduced. CPTED, as a security principle, provides a robust approach to the design and maintenance of the built environment.

## **Response**

Lastly, physical security can use technical solutions to aid response efforts after a threat is identified. Incident response system is a structured methodology for handling security events (incident, compromise and breach).

### **Incident Response Plan**

An incident response plan ensures that in the event of a security breach, the right personnel, procedures and technology are in place to effectively deal with a threat.

**Objectives:**

- Having an incident response plan in place ensures that a structured investigation can take place to provide a targeted response to contain and remediate the threat.
- Defines the team structure and process that the organization will follow when an incident occurs.
- Outline executive support and oversight of the process, as well as key stakeholders.
- Aims to reduce the costs of incidents and the associated response through a well-organized strategy for managing security event.

**Incident Response Plan Components:**

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Lesson Learned

Every company should have a written incident response plan and it should be accessible to all employees. Incident response plans should be specific to different incident types. For example, an incident response plan for a physical security breach, such as a break-in, would be very different from a data breach or cyber incident response plan.

## **Personnel Tracking**

*“Personnel tracking”* is most important in high-security environments, like corrections centers. Any facility at high risk of experiencing violence or of becoming the target of an attack must instantly identify the locations of security personnel for rapid response. A guard tour system is one kind of solution that monitors personnel movement in real time to ensure maximum readiness.

## **Evacuation Management**

Fires, natural disasters, and other emergencies require an immediate response from all parts of your organization to ensure your personnel's safety. Managing evacuations is one of the most important parts of emergency management. Automated emergency mustering and roll call systems verify whether personnel are safe at muster points or still at risk inside your facility. This information helps emergency managers and first responders act more effectively during chaotic and dangerous circumstances.

## **Security Operations Center –SOC**

A Security Operation Center (SOC) is a centralized function within a corporate security management or architecture employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing,

detecting, analyzing, and responding to all security incidents. It is popularly known as Security Control Room.

Also, it is a security command center.



A SOC acts like the hub or central command post, taking in telemetry from across an organization's security deployments, including its facilities, remote sites, personnel, and stakeholders, wherever those assets reside. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored and analyzed. For each of these events (guard patrols/SITREP, access control/alarms log, CCTV footages) the SOC must decide how they will be managed and acted upon.

SOCs operate 24-7 with employees working in shifts. A

SOC can be built internally, alternatively entirely or partially outsourced to external providers.

Security Operations Center (SOC) form the hub of a site's security, continuously receiving information from a range of security staff and systems. Whether designing a new SOC from scratch or looking to improve an existing SOC, consideration should be given to the following features:

- People
- Physical design
- Implementation
- Systems
- Policies/Procedures
- Resilience
- Response

## **Benefits of SOC**

The primary benefit of having a SOC is the improvement of security incident detection through continuous monitoring and analysis of people interactions with security measures and intelligence findings. By analyzing activities across the organization's security architectures around the clock, SOC teams can detect and respond to security incidents early. This is crucial, as time is one of the most critical elements in an effective security incident response.

CSO sleeps but SOC does not sleep nor slumber!

The 24/7 SOC monitoring gives organizations a significant advantage in the struggle to defend themselves against incidents and intrusions regardless of source, time of day, or type of attack. The gap between the attacker's time to compromise and the time to detect decreases, which helps organizations stay on top of threats facing their environments and limit their risk.

SOC operatives continuously manage known and existing threats while working to identify emerging risks.

The key benefits of a SOC include:

- Uninterrupted monitoring of events and remote supervision of security system deployments
- Improved incident response times and incident management practices
- Decreased gap between the time of compromise and the time to detect
- Software and hardware assets are centralized for a more holistic approach to security
- Effective communication and collaboration to detect and classify adversarial tactics and techniques.
- Reduction of costs associated with security incidents
- More transparency and control over security operations

## **Building Security Operations Center**

Before you begin your journey of building out an effective SOC, you should first know the essentials. This entire process will revolve around people, processes, and technology, as they all go hand in hand.

Key to the success of critical decision-making is the functional design of the SOC itself. Creating this environment begins with an information exchange with utility personnel who clearly understand the process, systems and applications of the control center environment. In addition to the physical components (e.g., work station and office location, lighting, acoustics, etc.), the software and other tools used by the operator must also be considered carefully.

The resultant design and solution set is one that best meets the needs of the trained personnel and their unique operating environment.

Within this design, there are four (4) critical factors or components to consider:

1. Spatial
2. Ergonomic
3. Environmental
4. Functional





## Seven Steps to Building your SOC

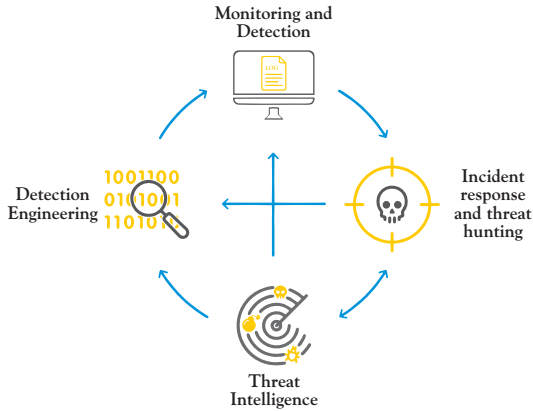
1. Develop your security operations center strategy
2. Design your SOC solutions
3. Create processes, procedures, and training
4. Prepare your environment
5. Implement your solutions
6. Deploy end-to-end use cases
7. Maintain and evolve your solutions

## Security Operation Center Deployment Model

There are several different ways for an organization to acquire SOC capabilities. The most common deployment models include:

- **Internal SOC:** In-house and dedicated
- **Managed SOC:** 3rd Party/out-tasked
- **Hybrid SOC:** Combination of dedicated and out-tasked

## Modern SOC Components



## Essential Tools/Equipment

- Ergonomic Furniture
- Communication Gadgets (Telephony and VHF Radio)
- CMS Software (Visual and Data)
- Uninterrupted Power Supply
- GPS/GPRS Tracking Solution
- Computers
- Physical Security System
- Internet Access Point

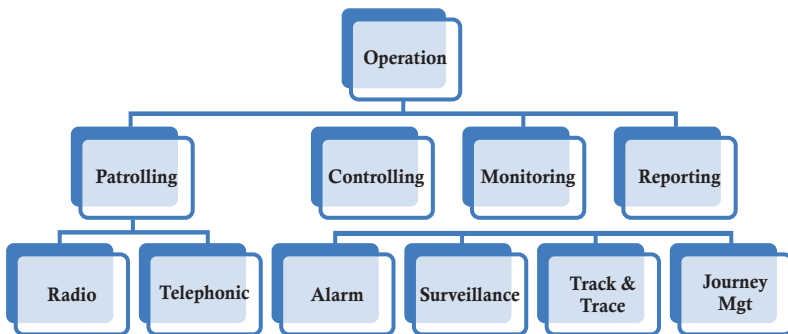
**An effective SOC operation depends on skilled people, specifically designed processes/procedures and technologies to;**

- Provide awareness of potential and imminent security threats

- Contain threats
- Coordinate emergency preparedness, response and recovery

## Design and Operations

1. Resources planning/ mapping
2. Setting up working environment
3. Implementing physical security mechanisms
4. Developing operational requirements & functions
5. Manpower sourcing
6. Training
7. Testing/Simulation/Drill



## Principles

The first thing to establish is that a working SOC is a professional space. It's not a space for people to come for a break or a conversation about the game. Access to the control room should be controlled and a list of authorized people clearly displayed.

## **Personnel Management**

The role of the security controller, SOC operator or whatever other name you wish to give that person requires specific skills and training. If the control room doesn't operate effectively this affects the entire security operations. The controller needs attention to detail and an ability to act under pressure. They also need to be aware of all working SOPs with their applications and must know where to find them in a hurry.

Operators should be able to demonstrate that appropriate human factors considerations have been given to the design, commissioning, and operation of SOC under both normal and abnormal plant operating conditions to reduce the frequency of human error due to control room deficiencies.

It is vitally important that SOC and its operators are considered as a whole system and not in isolation of each other. For example a well-designed SOC for use by 4 operators is dangerous when staffed by 3 operators. Similarly, the best-trained operators cannot guarantee high reliability in a poorly designed SOC.

## **Core Skills for SOC personnel**

- Customer Oriented
- Computer Literate
- Ethical Behaviour
- Initiative

- Orientation to Work
- Personal Growth
- Consistency and Reliability
- Deadlines –On time
- Process Improvement
- Analytical



Section

# 5

## IT SECURITY



*IT security incorporates both cybersecurity and infosec but refers specifically to the protection of digital data and the security maintenance of the computer systems and networks that store it.*

*This section explains basics knowledge of keeping digital data safe from internal and external threats*



MAKING SENSE OF SECURITY



# IT SECURITY

## *Introduction*

**T**he foundation for security is assets that need to be protected. Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information technology (IT) is a concept that refers to digital technology, i.e. hardware and software for creating, collecting, processing, storing, transmitting, presenting and duplicating information. The information may be in the shape of; **sound, text, image or video.**

Hence, IT means a merging of the traditional areas of computers, telecom and media. The phrase IT security is often used interchangeably with cybersecurity and information security (infosec). An Information System is much more than computer hardware. It is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource within and outside the organization.

**IT Artefacts:** Supporting resources to manage information

1. Personal computers
2. Networks
3. Operating systems and applications constitute
4. Human (People)
5. Tools (electronic – digital/analogue and non-electronic)

To protect the information and its related systems from danger, tools, such as policy, awareness, training, education, and technology are necessary.

## **Types of IT Security**

There's no such thing as a general IT security strategy. Every organization must quantify the specific risks to its IT networks and work out where to concentrate its efforts and resources. That process involves evaluating the following security threats individually.

- **Network Security**

Network security is required to protect your hardware and software networks from unauthorized access. In many ways, it's the most significant strand of IT security to consider as it's these networks that contain the data any IT security strategy is designed to protect.

Good network security should ensure that your network remains safe and reliable to operate within and is secured against attacks.

### **Types of Network Security Solutions, Devices, and Tools**

1. Firewalls
2. WAN and Branch Protection
3. Intrusion Prevention System (IPS)
4. Secure Web Gateway
5. SSL Inspection
6. Cloud On-ramp
7. Virtual Private Network -VPN
8. Perimeter Security
9. Network Automation
10. Compliance

- **Cybersecurity**

Cybersecurity, also sometimes referred to as internet/cloud security, concerns the protection of data that is sent or received over

the internet. Cybersecurity software, like antivirus and firewalls, monitors internet traffic for suspicious activity, blocking anything deemed malicious or alerting security teams to its presence.

With so many services now migrating to public i.e. software-as-a-service (SaaS), private, or hybrid cloud computing platforms, these virtual gateways are becoming ever-popular entry points for internet crooks. Always ensure to protect your files, devices and wireless networks (use at least WPA2 encryption).

Specific security protocols exist to protect cloud services including cloud data encryption, cloud access security brokers (CASB), cloud-based unified threat management (UTM), and more.

- **Application Security**

Application security, at a development level, refers to the measures taken to ensure apps have adequate security protocols coded into them and don't contain any vulnerabilities that could later be exploited.

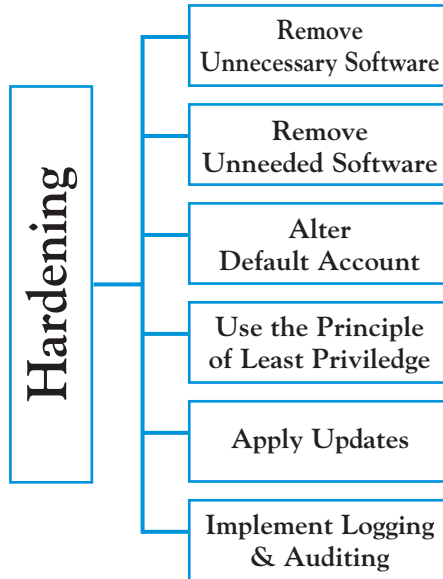
**Key information**

*A “zero-day vulnerability” is a security flaw present in a software program or operating system that doesn't have a working fix and which is usually unknown to developers.*

Hackers are constantly on the hunt for such vulnerabilities to exploit.

## Operating System Hardening

When we look at operating system hardening, we arrive at a new concept in information security. One of the main goals of operating system hardening is to reduce the number of available avenues through which our operating system might be attacked. The total of these areas is referred to as our attack surface. The larger our attack surface is, the greater chance we stand of an attacker.



- **Endpoint Security**

In many ways, end users are the most difficult security threats to mitigate. Every individual user is capable of jeopardizing the security of a network, whether that's through allowing malicious viruses in or letting sensitive information out.

Endpoint security measures cover every vulnerable point an end-user may come into contact with, including computers, mobiles, other IoT devices, email clients, or any user-dependent network gateway.

First and foremost, endpoint security concerns the process of securing individual devices and user-controlled entry or exit points.

There are several ways to prevent end-users from allowing malicious content to enter a network, including the use of a Virtual Private Network (VPN), sophisticated anti-malware, training so users are aware of cyber threats like phishing, and the application of software to prevent the usage of breached credentials.

### **Information Security Objectives –CIA Triad**

Security concerning IT and information is normally defined by three aspects, or goals; confidentiality, integrity and availability. The concepts can be seen as the objectives with security regarding IT and information and are often referred to as the '**CIA triad**'. The C.I.A. triangle has been considered the industry standard for security since the development of the mainframe.

- **Confidentiality:** Prevention of unauthorized disclosure or use of information assets
- **Integrity:** Prevention of unauthorized modification of information assets
- **Availability:** Ensuring of authorized access of information assets when required



**Two additional objectives:**

**a. Authenticity:** Authenticity means being genuine and able to be verified or trust. In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.

**b. Accountability:** Accountability involves actions of an entity can be traced uniquely to that entity, supports nonrepudiation, deterrence, fault isolation, intrusion, detection and prevention. Non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.



## **Threats against Information Assets**

Threat is something that potentially can impair the CIA triad in the future. That means that a threat consists of a potential action or occurrence that may affect the information asset's CIA triad negatively.

Information assets may be exposed to threats with the following potential actions;

1. An indication that an undesirable event may occur
2. Any potential danger to information or system
3. Circumstances that have the potential to cause loss or harm

Therefore, threats in this case are potential undesirable actions or occurrences, that performs or causes by actors, by human created artifacts or natural phenomena and which are supposed to impair the CIA triad of current information assets.

## **Attacks**

Attack is simply an attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems. The security attacks aim to compromise the CIA Triad.

## Types of Attacks

<b>Confidentiality</b>	<ul style="list-style-type: none"> <li>• <b>Interception</b></li> </ul>
<b>Integrity</b>	<ul style="list-style-type: none"> <li>• <b>Interruption</b></li> <li>• <b>Modification</b></li> <li>• <b>Fabrication</b></li> </ul>
<b>Availability</b>	<ul style="list-style-type: none"> <li>• <b>Interruption</b></li> <li>• <b>Modification</b></li> <li>• <b>Fabrication</b></li> </ul>

## Incidents and Damages

While a threat is an assumption that an undesirable event may occur in a future, the term incident refers to the actual occurrence of such event. In other words, a threat may be realized as one or several incidents.

A threat may still exist after a realization, since underlying causes still may have capabilities to realize the threat several times. The probability for realization will however often decrease since people often increase the protection against realized threats. Like threats, an occurred incident may be unknown. Such incidents may be discovered after a while or remain unknown. Incidents that are realized by unknown threats are unexpected incidents. Incidents may lead to consequences. If a consequence affects the CIA triad of information assets uncontrolled and negatively, it is labeled as damage. There may be incidents that not

impair the CIA triad, for example a virus that infects or attacks an information system without causing any damage

Damages are uncontrolled impairs of the CIA triad of information assets.

### **Some Common Security Attacks**

**1. Attacks Threatening Confidentiality:** In general, two types of attack threaten the confidentiality of information: snooping and traffic analysis. Snooping refers to unauthorized access to or interception of data. Traffic analysis refers other types of information collected by an intruder by monitoring online traffic.

**2. Attacks Threatening Integrity:** The integrity of data can be threatened by several kinds of attack: modification, masquerading, replaying and repudiation.

**3. Attacks Threatening Availability:** Denial of service (DOS) attacks may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. They might make the system so busy that it collapses, or they might intercept messages sent in one direction and make the sending system believe that one of the parties involved in the communication or message has lost the message and that it should be resent.

## Security Mechanisms

Security mechanisms are something that will improve the CIA triad of information assets, that is; increase the information security.

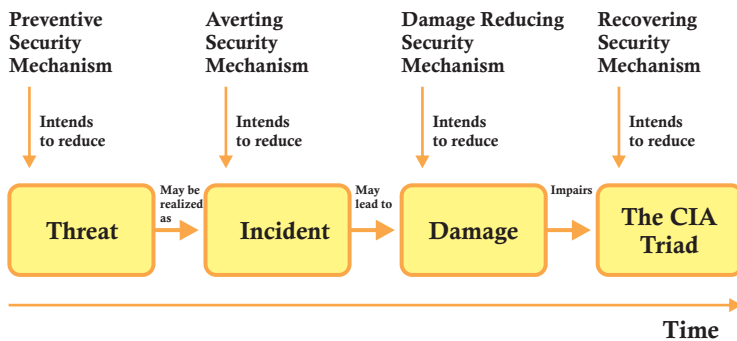
The terms protections, countermeasures, controls and safeguards may be used as synonyms to security mechanisms. Security mechanisms can be categorized in several ways. Bases for categorizations may be for example their relation to the CIA triad or what they consists of – e.g. hardware, software and policies.

Security mechanisms can be;

1. Preventing
  2. Averting
  3. Damage Reducing
  4. Recovering
- **Preventing Security Mechanisms** are highly directed to the threat; to affect threat agents with the aim to reduce the danger of a threat, or the probability that a threat will be realized to incidents. Examples of preventing security mechanisms are security awareness and laws.
  - **Averting Security Mechanisms** intend to obstruct incidents, e.g. in the shape of firewalls or encryption programs.
  - **Damage Reducing Security Mechanisms** ensure to bridge the missing link between threat,

incident, damage and CIA e.g. use of fire extinguisher.

- **Recovering (or Restoring) Security Mechanisms** recover already damaged information assets. An example of a security mechanism is anti-virus software that repairs infected files.



Summing up, a categorization of security based on time of an incident consists of four categories: preventing, averting, damage reducing and recovering security mechanisms.

## Vulnerability

Vulnerability is absence of security mechanisms, or weaknesses in existing security mechanisms. Vulnerability might be a specific operating system or application that we are running, a physical location where we have chosen to place our office building, a

data center that is populated over the capacity of its air-conditioning system, a lack of backup generators, or other factors.

## Risk

Risk is another fundamental concept in the area of security. Risk is the likelihood that something bad will happen. In order for us to have a risk in a particular environment, we need to have both a threat and a vulnerability that the specific threat can exploit. For example, if we have a structure that is made from wood and we set it on fire, we have both a threat (the fire) and a vulnerability that matches it (the wood structure). In this case, we most definitely have a risk.

Risk is someone's estimation concerning the occurrences of incidents and potential damages caused by incidents.

Consequently, the concept of risk consists of two parts; the probability or the expected frequency of that an incident will occur and the potential damages an incident may cause.

**This can be expressed in the following equation:**

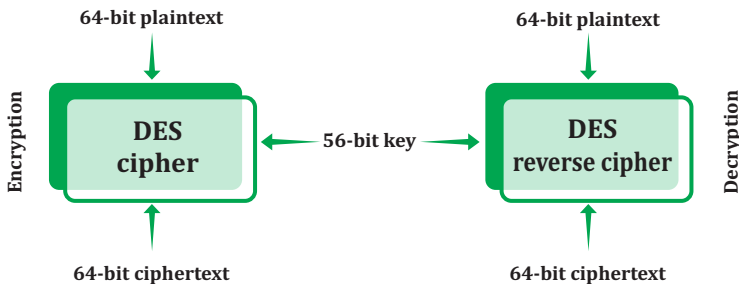
**$R = L \times P$**  (R stands for risk, L is potential loss,  
and P is probability or expected frequency of loss)

Even if an incident leads to a serious damage, there is no risk if the probability or expected frequency is zero, and reverse. *This means that  $R = 0$  require  $L = 0$  and/or  $P = 0$ .*

## Techniques of Information Security

### Cryptography

Cryptography, a word with Greek origins, means “*secret writing*”. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage. Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user, this process is called encryption. The original message is referred to as plaintext and the message that is sent through the channel is referred to as the cipher text. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.



**Traditional Ciphers:** Traditional ciphers used two techniques for hiding information from an intruder: substitution and transposition.

**Substitution Ciphers:** A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

**Transposition Ciphers:** A transposition cipher does not substitute one symbol for another; instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext, while a symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

**Modern symmetric-key ciphers:** Since traditional ciphers are no longer secure, modern symmetric-key ciphers have been developed. Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a cipher text from a plaintext. Modern ciphers are bit-oriented (instead of character-oriented). The plaintext, cipher text and the key are strings of bits.



---

## **Two modern symmetric-key ciphers are DES and AES**

**DES (Data Encryption Standard):** The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. It uses 56-bit symmetric key, 64-bit plaintext input. DES has been the most widely used symmetric-key block cipher since its publication.

**AES: (Advanced Encryption Standard):** The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the US National Institute of Standards and Technology (NIST) in 2001 in response to the shortcoming of DES. It processes data in 128 bit blocks and 128, 192, or 256 bit keys.

**Asymmetric-Key Cryptography:** Asymmetric-key cryptography is used for confidentiality. Unlike symmetric-key cryptography, there are distinctive keys in asymmetric-key cryptography, a private key and a public key. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with the corresponding private key. Both symmetric-key and asymmetric-key cryptography will continue to exist in parallel.

The conceptual differences between the two systems are based on how these systems keep a secret. In symmetric-

key cryptography, the secret token must be shared between two parties. In asymmetric-key cryptography, the token is unshared each party creates its own token. It is believed that both are complements of each other.

The advantages of one can compensate for the disadvantages of the other.

**Message Integrity (Hash Function):** There are occasions on which we may not even need secrecy, but instead must have integrity. One way to preserve the integrity of a document was traditionally through the use of a fingerprint.

The electronic equivalents of the document and fingerprint pair are the message and digest pair. To preserve the integrity of a message, the message is passed through an algorithm called a cryptographic hash function. The function creates a compressed image of the message that can be used like a fingerprint. To check the integrity of a message or document, we run the cryptographic hash function again and compare the new message digest with the previous one. If both are the same, we are sure that the original message has not been changed.

**Digital Signatures:** We are familiar with the concept of a signature. Digital signature is a Cryptographic technique analogous to hand-written signatures. A person signs a document to show that it originated from him/her or was approved by him/her. The signature is

proof to the recipient that the document comes from the correct entity. In other words, a signature on a document, when verified, is a sign of authentication – the document is authentic.

An electronic signature can prove the authenticity of the sender of the message. We refer to this type of signature as a digital signature. In Digital signature process the sender uses a signing algorithm to sign the message. The message and the signature are sent to the recipient. The recipient receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted, otherwise it is rejected. A digital signature needs a public-key system. The signer signs with her private key, the verifier verifies with the signer's public key. A cryptosystem uses the private and public keys of the recipient; a digital signature uses the private and public keys of the sender.

## Web Security

**Basic Authentication:** It is a simple user ID and password-based authentication scheme, and provides to identify which user is accessing the server and to limit users to accessing specific pages.

**Secure Socket Layer (SSL):** Netscape Inc. originally created the SSL protocol, but now it is implemented in World Wide Web browsers and servers from many

vendors. SSL provides the Confidentiality through an encrypted connection based on symmetric keys and authentication using public key identification and verification, connection reliability through integrity checking.

**Distributed Authentication - KERBEROS:** Kerberos is a network authentication protocol which Provides authentication for client-server applications, and data integrity and confidentiality. It relies entirely on symmetric cryptography. In this when Client wants service from a particular server an Authentication Server allows access based on tickets. Ticket specifies that a particular client (authenticated by the Authentication Server) has the right to obtain service from a specified server. In this the network is under the control of an Authentication Server. This uses two types of tickets with two different lifetimes. One ticket grants to right to ask for service which performed once per login session Ticket. For each type of service, use a ticket that grants the right to use that particular service Ticket. Every time that service is needed, the ticket is used.

## Protecting IP

**IPSEC:** IPSEC is an Internet standard for ensuring secure private communication over IP networks, and it was developed by IPSEC working group of IETF. It

implements network layer security by facilitating direct IP connectivity between sensitive hosts through untrusted networks.

## Access Control

**Firewalls:** Firewall isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others. A firewall is used to control traffic flow between networks.

### Firewall uses the following techniques

**Packet Filters:** It is the commonly used firewall technique which Operates at IP level, Checks each IP packet against the filter rules before passing (or not passing) it on to its destination.

In this internal network connected to Internet via router firewall that filters packet-by-packet, decision to forward/drop packet based on source IP address, destination IP address, TCP/UDP source and destination port numbers, ICMP message type, TCP SYN and ACK bits. It is Very fast than other firewall techniques but Hard to configure.

**Application Gateways:** Application gateways Filters packets on application data as well as on IP/TCP/UDP fields and allow select internal users to telnet outside. In this all telnet users require to telnet through gateway, for authorized users, gateway sets up telnet connection to

destination host and Gateway relays data between 2 connections. Router filter blocks all telnet connections not originating from gateway.

Conclusively, each information security technique has its unique features and applicability. To ensure information security the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information.

Section

# 6

## SECURITY ANALYTICS

### *Forecasting & Crime Prediction*



*Nowadays, crimes are increasing at a high rate which is a great challenge not only for security agencies but for every human and business establishment.*

*A huge amount of data on different types of crimes or security activities at different geographical time and locations is collected and stored daily even as simple as visitor log. It is highly essential to analyze data so that potential measure for mitigating crime incidents and predicting similar incident patterns for future becomes possible.*





# BIG DATA

ADVANCED ANALYTICS  
VISUALIZATIONS



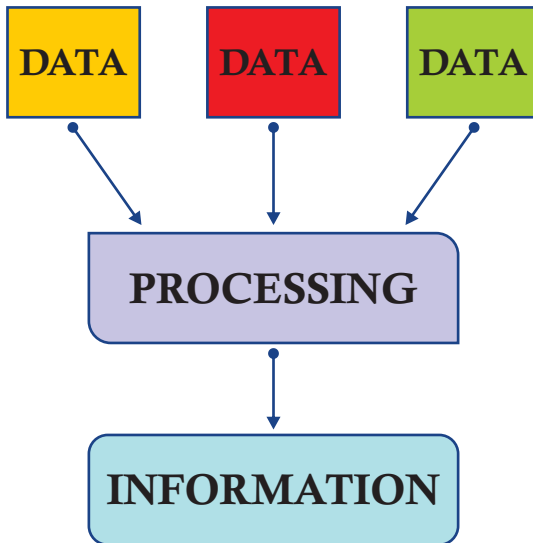
# WHAT IS DATA?

**T**oday in our rapidly changing world, tons and tons of data are being stored every second all around the world. Data could be reflex human activity, thoughts, mood, intent, desire, etc. This helps us predict what could possibly be the other person next action and prepare ourselves in advance when data is processed into information. It is the more reason why from the past until now, that those who held the most information could easily prevail over those who don't.

## What is DATA?

Today in our rapidly changing world, tons and tons of data are being stored every second all around the world. Data could be reflex human activity, thoughts, mood, intent, desire, etc. This helps us predict what could possibly be the other person next action and prepare ourselves in advance when data is processed into information. It is the more reason why from the past until now, that those who held the most information could easily prevail over those who don't.

This leads to the saying that *“Information is power”*.



## Data

- It comes from a Latin word, **datum**, which means *"To give something."* Over a time *"data"* has become the plural of datum.
- It is a raw and unorganized fact that required to be processed to make it meaningful.
- It can be simple at the same time unorganized unless it is organized.
- It comprises facts, observations, perceptions numbers, characters, symbols, image, etc. in a raw form.
- It is always interpreted, by a human or machine, to derive meaning. Therefore, data is meaningless.

## Big Data

Big data is a process that somewhat similar to waking up what that is to be compared to the best teacher of all, *"Experience"*, but in the case the experience which comes in the form of information. **Big data** is a term that describes the large volume of data – both structured and unstructured. Also, it is a term used to describe a collection of data that is huge in size and yet growing exponentially with time.

Big data is a system which digs down in to the data set to look for potentially useful hidden patterns.

## Data Analytics



The term data analytics refers to the process of examining datasets to draw conclusions about the information they contain. Data analytic techniques enable you to take raw data and uncover patterns to extract valuable insights from it.

Gone are the days when crimes are fought atop of horses to save the day. In this day and age, we need weapons of a different kind to battle crime. Data, algorithms, analytics – these are the newest addition to help law enforcement officials and organisation to protect lives and properties. **'Predictive policing'** is the art of predicting crimes before it takes place. It's not about apprehending the right individuals, but about preventing the crime.

*Big Data Analytics is helpful in predicting the kind of crimes an area might be susceptible to at any given time.*

Maybe burglaries will be more prevalent in a certain neighborhood during a particular time period and so on.

As the process of analyzing raw data to find trends and answer questions, the definition of data analytics captures its broad scope of the field. However, it includes many techniques with many different goals. The data analytics process has some components that can help a variety of initiatives. By combining these components, a successful data analytics initiative will provide a clear picture of where you are, where you have been and where you should go.

The goal of big data analytics is to automatically detect patterns of crime.

### **Benefits of Big Data Analytics**

1. Decision-Making Improvement
2. Identify and reduce inefficiencies
3. Remove fraud and abuse
4. Reducing crime and security threats
5. Maintains transparency in service

### **Types of Data Analytics**

There are four primary types of data analytics: descriptive, diagnostic, predictive and prescriptive analytics. Each type has a different goal and a different place in the data analysis process.

- **Descriptive analytics** helps answer questions

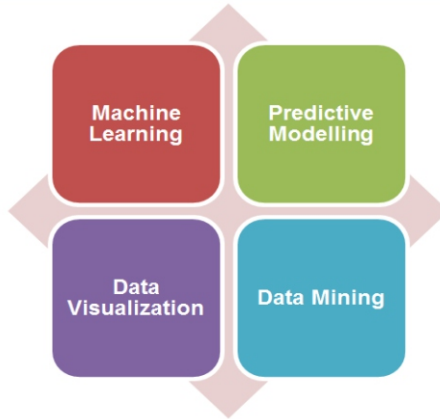
- about what happened.
- **Diagnostic analytics** helps answer questions about why things happened.
- **Predictive analytics** helps answer questions about what will happen in the future.
- **Prescriptive analytics** helps answer questions about what should be done.

## Data Analytics Technology

The big data analytics technology is a combination of several techniques and processing methods. Big data analytics examines large amounts of data to uncover hidden patterns, correlations and other insights. With today's technology, it's possible to analyze your data and get answers from it almost immediately – an effort that's slower and less efficient with more traditional operation intelligence solutions.

There's no single technology that encompasses big data analytics. Of course, there's advanced analytics that can be applied to big data, but in reality several types of technology work together to help you get the most value from your information.

Here are the few ones more applicable to security profession:



These technologies are based on the simple fact that humans are creatures of habit. No matter how much we might like to deny it, we stick to patterns and our preferences.

***Human being rarely strays from the known.***

To oversimplify it, data is collected from public records, social media, and other sources of information and algorithms are used to determine the probability of the crime – the geographical location, approximate time, demographic – and action is taken accordingly.

***Think like a criminal to catch a criminal.***

Criminals are coming up with ingenious ways to commit crimes but we have shiny new armor to combat

it in the form of technology. It's to be expected that it will get shinier with the advancements in technology.

Integrating Big Data Analytics and Physical Security technologies is the way forward as it has yielded concrete positive results.

## **Predictive Analytics Models**

The amalgamation of an increasingly complicated world, the vast proliferation of data and the pressing desire to stay at the forefront of competition have prompted organisations to focus on using analytics for driving strategic business decisions. Rather than *“going with intuition”* when making critical and strategic decisions, organisations are embracing analytics and systematic statistical reasoning to make decisions that improve efficiency, risk management and even profits. Smarter decisions are powered by predictive analytics.

In an era where data has now become the new oil, it is paramount to have the right techniques, models and tools for processing the numerous (2.5 quintillion bytes) of data produced regularly. Predictive data analytics is a technology that can anticipate future trends. It is an evolution of earlier data analytics models and works by predicting what will happen in the future by analyzing historical data, discovering patterns and using that information to draw up predictions about the overall direction of the industry.



Predictive analysis models and findings are powered by machine learning and artificial intelligence.

**Fraud detection and security** – Predictive analytics can help stop losses due to fraudulent activity before they occur. By combining multiple detection methods – business rules, anomaly detection, predictive analytics, link analytics, etc. – you get greater accuracy and better predictive performance. And in today's world, cybersecurity is a growing concern. High-performance behavioral analytics examines all actions on a network in real time to spot abnormalities that may indicate occupational fraud, zero-day vulnerabilities and advanced persistent threats.

## **Types of predictive models**

Predictive analytics models are not a monolith. There are different models developed for design-specific functions.

### **1. Forecast Models**

A forecast model is one of the most common predictive analytics models. It handles metric value prediction by estimating the values of new data based on learnings from historical data. It is often used to generate numerical values in historical data when there is none to be found. One of the greatest strengths of predictive analytics is its ability to input multiple parameters. For this reason, they are one of the most widely used

predictive analytics models in use. They are used for crime prediction and business purposes.

## **2. Classification Models**

One of the most common predictive analytics models are classification models. These models work by categorizing information based on historical data. Classification models are used in different industries because they can be easily retrained with new data and can provide a broad analysis for answering questions. Classification models can be used in different industries like finance and retail, which explains why they are so common compared to other models.

## **3. Outliers Models**

While classification and forecast models work with historical data, the outliers model works with anomalous data entries within a dataset. As the name implies, anomalous data refers to data that deviates from the norm. It works by identifying unusual data, either in isolation or in relation with different categories and numbers. Outlier models are useful in industries where identifying anomalies can save organisations millions of dollars, namely in retail and finance. One reason why predictive analytics models are so effective in detecting fraud is because outlier models can be used to find anomalies. Since an incidence of fraud is a deviation from the norm, an outlier model is more likely to predict it before it occurs. For example, when identifying a fraudulent transaction (FORENSIC), the

outlier model can assess the amount of money lost, location, purchase history, time and the nature of the purchase. Outlier models are incredibly valued because of their close connection to anomaly data.

#### **4. Time Series Model**

While classification and forecast models focus on historical data, outliers focus on anomaly data. The time series model focuses on data where time is the input parameter. The time series model works by using different data points (taken from the previous year's data) to develop a numerical metric that will predict trends within a specified period.

#### **5. Clustering Model**

The clustering model takes data and sorts it into different groups based on common attributes. The ability to divide data into different datasets based on specific attributes is particularly useful in certain applications, like marketing. For example, marketers can divide a potential customer base based on common attributes. It works using two types of clustering – hard and soft clustering. Hard clustering categorizes each data point as belonging to a data cluster or not, while soft clustering assigns data probability when joining a cluster.

## **Creating predictive algorithm models**

While developing a predictive analytics model is no

simple task, we managed to break down the process to six essential steps.

**Stage 1: Defining scope and scale** – Determine the process that will use the predictive analytics models and what the desired business outcomes will be.

**Stage 2: Profile data** – Predictive analytics is data-intensive. So the next step is to explore the data needed for analysis. Organisations have to decide where it is stored, its current state, and how accessible will it be.

**Stage 3: Gather, cleanse and integrate data** – Once data is found, it needs to be cleaned and gathered. It is an important step because predictive analytics models need a strong foundation to work effectively.

**Stage 4: Incorporate analytics into the business process** – The model can only be used to integrate it into the business process to get the best outcomes.

**Stage 5: Monitor models and measure the business results** – The model needs to be measured to see if it makes genuine contributions to the overall security need or business processes.

## **Limitations of predictive analytics models**

Despite the immense economic and security benefits of predictive analytics models, they are not fool-proof, fail-safe models. There are some disadvantages to predictive analytics. Predictive models need are specific set of

conditions to work, if these conditions are not met, then it is of little value to the organisation.

### **1. The need for massive training datasets**

For predictive analytics models to be successful at predicting outcomes, a huge sample size representative of the population is required. Ideally, the sample size should be in the high thousands to a few million. If datasets are smaller than the predictive analytics models will be unduly influenced by anomalies in the data, which will distort findings. The need for massive datasets inevitably locks out a lot of small to medium-sized organisations who may not have this much data to work with.

### **2. Properly categorizing data**

Predictive analytics models rely on machine learning algorithms, and these algorithms can properly assess data if it is labeled properly. Data labeling is a particularly demanding and meticulous process because it needs to be accurate. Incorrect classification and labeling can cause several problems, like poor performance and accuracy in findings.

### **3. Applying learnings to different cases**

Data models have a problem with generalizability, which is the ability to transfer findings from one case to another. While predictive models are effective in their findings for one case, they often struggle to transfer their findings to a different situation.

## **Future of Security: Convergence**

It is becoming more and more important to keep up to date with not only cybersecurity but also physical security. Rapid technological innovations are changing our present and our perspectives for the future. The innovative technologies such as IoT, machine learning, artificial intelligence, and big data have revolutionized the way organizations conduct business in the digital landscape.

## **Security Risks – How they're changing**

More and more physical objects are gaining internet connection. It's not just our computers anymore; it's our cars, phones and even fridges. This is likely to present a greater risk to personal security in the future, because where there is internet connectivity, there's a chance for breach. This is why it is becoming more and more important to keep up to date with not only cyber security but also physical security.

## **What's next?**

In today's world, the lines between physical and digital are rapidly blurring together. Nowhere is this more evident than in the security world. Where once there was cybersecurity staff protecting networks and physical security staff securing physical assets, today these worlds are colliding. From digital cameras to

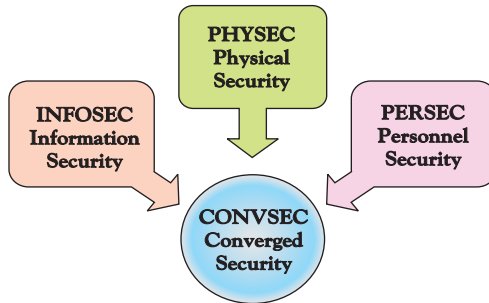
biometric access systems and network driven enterprises, the cyber and physical security worlds are really crashing together.

Really and truly, it's clear that threats to our security are increasing. This can be largely attributed to the growth of cybercrime. But don't forget, cybercrime doesn't just threaten your data. With more and more personal items subject to cybersecurity threats, it is becoming a personal threat to you and your home. It is therefore important that physical security is not neglected, and is good way to ensure a peace of mind. –**Converged Security!**

## Security Convergence

Security convergence refers to the integration of the collective security resources of an organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings which is to be achieved in a collaborative and strategic manner.

Also, Converged Security is a new way of viewing all risks that face an organisation, combining risks from the Physical, IT/Cyber, and Personnel disciplines within an Enterprise Security Risk Management (ESRM) model that delivers uniform Governance over an organisation.



The key concepts of security convergence include both the IT security and physical security. Converged security efforts require attention to both '**technology integration**' and '**interoperability**', as well as organizational readiness to improve people's and teams' collaboration.

The point where physical and IT security risks connect or cross over in an organization is commonly referred to a convergence point (link). It is essentially the area where the organization is often most vulnerable. As a result, all of your traditional security silos (Physical, Information and Personnel) need to be viewed as part of a **bigger strategy** aligned with your organisation's goals and mission.

To avoid weak link, we need to look at all attack vectors to ensure appropriate levels of mitigation that are deployed to reduce the overall risk. There is need to work holistically to eliminate grey areas between controls, as attackers will continue to look for and



exploit the weakest link.

A recent ASIS Foundation survey found that while 20% of respondents cited cost saving as a factor that might convince them to converge, only 7% of those who did converge cited it as a primary benefit. The bigger benefits realized were *“Better alignment of security strategy with corporate goals”* (40%), *“Enhanced communication/cooperation”* (39%), and *“Shared practices/goals across functions”*(35%).

## Enterprise Security Risk Management - ESRM

ESRM is the management of any security risk using established risk principles. There are five core risk principle elements:

1. Identify your assets
2. Identify risks associated with those assets
3. Mitigate those risks
4. Respond to incidents
5. Continue learning from incidents by being situationally aware

Risk is a very broad term, and ESRM deals, quite specifically with '**security risk**'.

A security risk in the context of ESRM is anything that threatens harm to the enterprise, its mission, its employees, customers, partners, its operations, or its

reputation. Security risks take many different forms, and new ones are being introduced all the time.

Recognizing those risks, making them known to the enterprise, and having a security resource assist business functions to mitigate them is central to the **ESRM** philosophy.

*Converging Threats = Converging Solutions*

## Converging Solutions

One of the key benefits of a converged security model is the ability to create a single pane of glass view (Security Operation Center -SOC) to capture all threats in real-time (DATA), monitored by a single first responder team 24x7.

For instance, in the ESRM framework this means using mitigations from multiple disciplines to monitor and mitigate risks; including placing guards, installing cameras, monitoring networks, and using digital and physical access controls.

The use of Artificial Intelligence (AI) is creating a new role for the legacy security camera, utilizing them to collect valuable information on customers and how they interact with your organisation.

Summarily, a Converged Security approach will ensure that organisation operates as securely as possible,

making the best use of scarce resources to protect lives and properties; as well as the organization's reputation and brand.

### *Moving forward!*

**Converged Security Product:** Adopting Risk-informed and Data-driven approach (**Analytics Modeling and Forecasting**). It is important to start taking advantage of innovations that evolve from the convergence of security products, which will lead to more cost effective and adaptive controls. Pull together data from multiple disparate systems including video analytics, access control, intrusion, GPS/GPRS tracking platforms, and more onto easy-to-read dashboards, allowing you to report on key metrics for your business and creating actionable business intelligence across your locations. By correlating information from multiple data points, you can help mitigate loss, optimize intelligence gathering, and improve profitability.

Realizing the full power of your data has never been easier!

Artificial Intelligence is a key example of this as it uses traditional physical security (cameras) combined with analytics to provide new benefits to your organisation, from facial recognition of staff and VIP customers, active market research opportunities, and enhanced

security profiling (confirming that the face matches the access card being presented).

Everyone knows that there is no single solution to security threats; no silver bullet; no magic product to solve problem of insecurities. Instead it requires a combination of elements, working in a consolidated strategy, to provide the best protection.



*Key information*

*As threats continue to evolve and adapt, so do the controls available to organisations to mitigate them.*

Security convergence is the next step in the evolution of security, bringing the best of all existing disciplines into a coordinated defense to provide the best future-focused protection for your organisation.

Section

# 7

## SAFETY VS. SECURITY



*Safety and Security are too often used interchangeably, as if they mean the same thing. This can be a losing premise or argument.*

*Practically, Safety and Security are two sides of the same COIN. What coin? The answer can be found in this piece.*

MAKING SENSE OF SECURITY





# SAFE OR SECURE

*“Safety is the condition or state of being free from harm or risk”.*

Unfortunately, when people think about security, they often equate it with safety. The primary definition of safety is apparently similar to that of security but inherently not the same. Perhaps the lingering differences between the words can be found in their differing etymologies.

- Safe comes from Latin *salvus*, “*uninjured, healthy.*” It’s related to *salus*, “*good health.*”
- Secure comes from Latin *securus*, “*without care,*” from *se*, “*free from,*” and *cura*, “*care.*”



*Key information*

*To be safe, can mean to be secure, but to be secure does not necessarily mean a person is safe.*

We install security systems on our homes for protection of lives and properties against intended threats. We add security alarms and tracking device to our vehicles in hopes that we deter theft. An alarm system cannot ensure an individual is protected from actual harm, just as a tracking device cannot prevent car accident.



*Key information*

*The relationship between safety and security is such that a weakness in security creates increased risk, which in turn creates a decrease in safety.*

As a result, safety and security are directly proportional, but both are inversely proportional to risk.

Think of SECURITY as if it were the overarching umbrella protecting SAFETY:





*Securing safety! Security surrounds, but safety enfolds.*

Safety and security are important terms that are associated with the protection of a person, organization, and properties against internal/external or unintended/intended threats that are likely to cause harm. Security seems to be the main aspect among the two terms because safety cannot be achieved if security is not guaranteed.

From the analysis above, it is clear that safety and security are two sides of the same coin known as THREAT.

### *Safe and Secure*

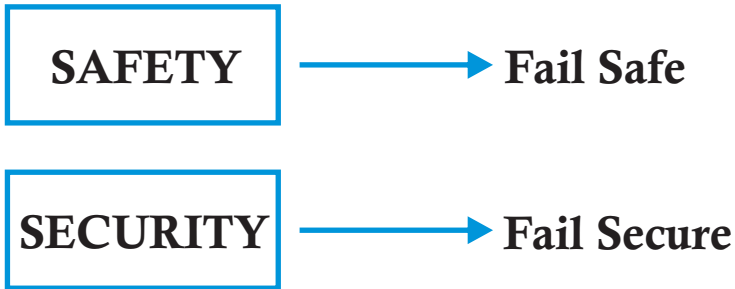
The integration of safety and security.

In a world where security threats appear to be

constantly evolving and resources are becoming more and more stretched, the integration of safety and security may be worthwhile on a number of levels, from improving understanding to the effective and efficient provision of security measures.

Safety and security practitioners have traditionally treated safety and security as different system properties. Both communities generally work in isolation using their respective terminologies and frameworks. Safety experts see their role as preventing losses due to unintentional actions by benevolent actors. Security experts see their role as preventing losses due to intentional actions by malevolent actors.

### Core Conflict



Safety stands for accident avoidance, and security for crime/loss prevention. The best way to explain it is to use an example for the above graphical illustration: If you think of an emergency exit, on the one hand you have the safety aspect. In safety terms you need to be

able to get out of the building at any time, and the door should preferably always be open. As far as security – with a focus on building protection – is concerned, this door would be permanently locked, so that no-one can get in.

However, since security and safety share the common aim of protecting people, safety-critical assets tend to be security-critical assets. Hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents. Then, having a common approach to security and safety would introduce consistency and, if integrated, would naturally identify and manage conflicts, as well as realizing efficiency and reliability. Developing effective security requires an ever greater understanding of the operations within a high hazard workplace in which critical assets are identified and proportional security measures are applied for their protection against a range of credible attack scenario.

Having security and safety departments merged since they share common protecting people and critical assets. Would it be effective, sustainable and economical?

### ***Stop and think***

Integrated Safsec! –The future of safety and security.

## Workplace Health and Safety Guide

Health and safety is a fundamental part of managing an organisation as it impacts on all functions within the organisation.

In general, the laws apply to all businesses, no matter how small. As an employer, or a self-employed person, you are responsible for health and safety in your business. You need to take the right precautions to reduce the risks of workplace dangers and provide a safe working environment.

If you think health and safety has to be complicated – it doesn't. All that's required is a basic series of tasks.

Key components of health and safety guide plan

- A reporting system
- Training programs
- Inspections
- Emergency planning
- Continuous improvement

## 10 Elements Approach

Simple and comprehensive approach to get you started in managing health and safety in your business.

**1. Decide who will help you with health and safety duties:** As an employer, you must appoint someone competent to help you meet your health and safety

duties. A competent person is someone with the necessary skills, knowledge and experience to manage health and safety. This could be;

- Yourself
- One or more of your workers
- Someone from outside your business

**2. Write a health and safety policy for your business:** Describing how you will manage health and safety in your business will let your staff and others know about your commitment to health and safety. This will be your health and safety policy. It should clearly say who does what, when and how. If you have five or more employees, you must have a written policy. The policy does not need to be complicated or time-consuming



Key information

**Note:** *A policy will only be effective if you and your staff follow it and review it regularly.*

### 3. Manage the risks in your business

You must manage the health and safety risks in your workplace. To do this you need to think about what, in your business, might cause harm to people and decide whether you are doing enough to prevent that harm. This is known as a risk assessment. You can check online for an assessment template to use.

Once you have identified the risks, you need to decide how to control them and put the appropriate measures in place. A risk assessment is not about creating huge amounts of paperwork, but rather about identifying sensible measures to control the risks in your workplace. The law does not expect you to remove all risks, but to protect people by putting in place measures to control those risks.

*How do I assess the risks in my workplace?*

A good starting point is to walk around your workplace and look for any hazards – a hazard is anything that may cause harm. Then think about the risks – a risk is the chance, high or low, of somebody being harmed by the hazard, and how serious the harm could be.

Think about how accidents could happen and who might be harmed. Ask your employees what they think the hazards are, as they may notice things that are not obvious to you and may have some good ideas on how to control the risks. Concentrate on the real risks – those that are most likely to cause harm. Consider the measures you are already taking to control the risks and ask if there is anything you should do to make your workplace safer.

Once you have identified the risks and what you need to do to control them, you should put the appropriate measures in place. Then record your findings.

#### **4. Consult your employees**

You have to consult all your employees on health and safety. This does not need to be complicated. You can do this by listening and talking to them about:

- Health and safety and the work they do;
- How risks are controlled;
- The best ways of providing information and training.

Consultation is a two-way process, allowing staff to raise concerns and influence decisions on the management of health and safety. Your employees are often the best people to understand risks in the workplace and involving them in making decisions shows them that you take their health and safety seriously.

#### **5. Provide training and information**

Everyone who works for you needs to know how to work safely and without risks to health. You must provide clear instructions, information and adequate training for your employees. Don't forget contractors and self-employed people who may be working for you and make sure everyone has information on:

- Hazards and risks they may face;
- Measures in place to deal with those hazards and risks;
- How to follow any emergency procedures.

Ask your employees what they think about training to

make sure it's relevant and effective. Keeping training records will help you to identify when refresher training might be needed.

The information and training you provide should be in a form that is easy to understand. Everyone working for you should know what they are expected to do. Health and safety training should take place during working hours and it must not be paid for by employees. There are many external trainers who will be able to help you with your training needs but effective training can often be done 'in house'.

## **6. Provide the right workplace facilities**

You must protect the safety and health of everyone in your workplace, including people with disabilities, and provide welfare facilities for your employees. Basic things you need to consider are outlined below.

### **Welfare facilities**

For your employees' well-being you need to provide:

- Toilets and hand basins, with soap and towels or a hand-dryer;
- Drinking water;
- A place to store clothing (and somewhere to change if special clothing is worn for work);
- Somewhere to rest and eat meals.



## Health issues

To have a healthy working environment, make sure there is:

- Good ventilation – a supply of fresh, clean air drawn from outside or a ventilation system;
- A reasonable working temperature (usually at least 16°C, or 13°C for strenuous work, unless other laws require lower temperatures);
- Lighting suitable for the work being carried out;
- Enough room space and suitable workstations and seating;
- A clean workplace with appropriate waste containers.

## Safety issues

To keep your workplace safe you must:

- Properly maintain your premises and work equipment;
- Keep floors and traffic routes free from obstruction;
- Have windows that can be opened and also cleaned safely;
- Make sure that any transparent (eg glass) doors or walls are protected or made of safety material.

## **7. Make arrangements for first aid, accidents and ill health**

### **First aid**

You must have first-aid arrangements in your workplace.

You are responsible for making sure that your employees receive immediate attention if they are taken ill or are injured at work. Accidents and illness can happen at any time and first aid can save lives and prevent minor injuries from becoming major ones.

Your arrangements will depend on the particular circumstances in your workplace and you need to assess what your first-aid needs are.

As a minimum, you must have:

- A suitably stocked first-aid box;
- An appointed person to take charge of first-aid arrangements;
- Information for all employees giving details of first-aid arrangements.

You might decide that you need a first-aider. This is someone who has been trained by an approved organisation and holds a qualification in first aid at work or emergency first aid at work.

### **Accidents and ill health**

Under health and safety law, you must report and keep a record of certain injuries, incidents and cases of work-

related disease.

Keeping records will help you to identify patterns of accidents and injuries, and will help when completing your risk assessment. Your insurance company may also want to see your records if there is a work-related claim.

### **8. Display the health and safety law poster**

If you employ anyone, you must display the health and safety law poster, or provide each worker with a copy of the equivalent pocket card. You must display the poster where your workers can easily read it.

### **9. Get insurance for your business**

If your business has employees you will probably need employers' liability insurance. If an employee is injured or becomes ill as a result of the work they do for you, they may claim compensation from you.

Employers' liability insurance will enable you to meet the cost of any compensation for your employees' injuries or illness. Only a few businesses are not required to have employers' liability insurance. If you have no employees, or are a family business and all employees are closely related to you, you may not need it.

### **10. Keep up to date**

Following news and events in your industry will help you keep your health and safety policies and risk

assessments up to date. You can access HSE news in the way that suits you best.

Workplace security can protect your business against theft, while as well guarding the safety of your personnel against incursions of violence.

*Bridge the gap – Integrate safety and security!*

**IF IT'S NOT SECURE, IT'S NOT SAFE!**

Section

# 8

## SECURITY-BY-DESIGN PRINCIPLES



*The field of security practice is very broad and there are many principles that need to be adhered to in order to achieve fit-for-purpose secured mechanisms or measures. Specific fundamental principles underlie the design and implementation of mechanisms for supporting security policies.*

*This section explains 20 key design principles to be adopted in developing sustainable, reliable, efficient, cost effective and robust security solutions*



## PRINCIPLE ONE



### **SECURITY MUST BE IN BALANCE WITH THE RISKS**

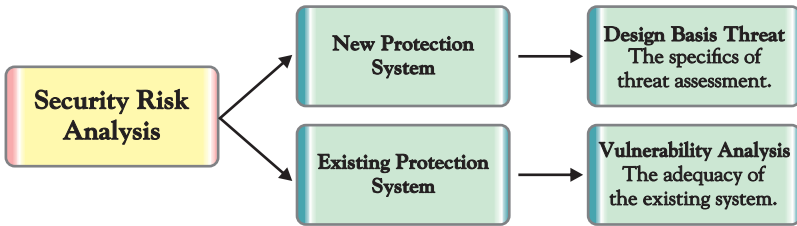
**C**omplete security risk analysis should be undertaken before security system design is being carried out. This will provide the raw material for the design-basis-threat using risk register. One of the objectives of these tasks is to ensure that the security measures deployed really do protect the enterprise against the most likely or most critical adversarial scenarios. It is very easy to deploy excessive or inadequate protection which is a waste of valuable resources and questionable competency.



*Key information*

*Most times, the root cause of security failures are often not a case of lack of budget, but not following a process that leads to the selection of the right and most efficient countermeasures pertinent to the risk.*

It is important to note that risk assessment helps to determine potential security risks for analysis.



**Security Risk Analysis (SRA)** is the first stage in the overall process of security risk management and it is an important corporate governance tool.



*Key information*

*Security risk analysis provides a methodology for assessing the likelihood of threats, usually malevolent, events and measuring that against potential impact and vulnerability.*

Specifically, the security risk analysis methodology or approach;

1. Identify assets and characterize the context in which they exist.
2. Identify potential threats (undesirable events) and assess them.



3. Estimate the likelihood of each threat.
4. Determine the potential impact to the asset if the threat occurs.
5. Plot impact and likelihood on a graph to determine a level of “raw” risk.
6. Measure the “raw” risk against vulnerability or controllability to determine protection priorities.

*Note: This process is cyclic and iterative.*

## SRA Chart

RISK	ADVERSARY	ASSET	ACTION	L	I	PRIORITY	CONTROL
R1	Burglars	Store Stocks	Theft of stocks	3	4	High	Baseline
R2	Local Youths	Business	Antisocial	3	2	Low	Barely
		Park	Behaviour	4	1	Negligible	Adequate
			Criminal				Barely
			Damage				Adequate

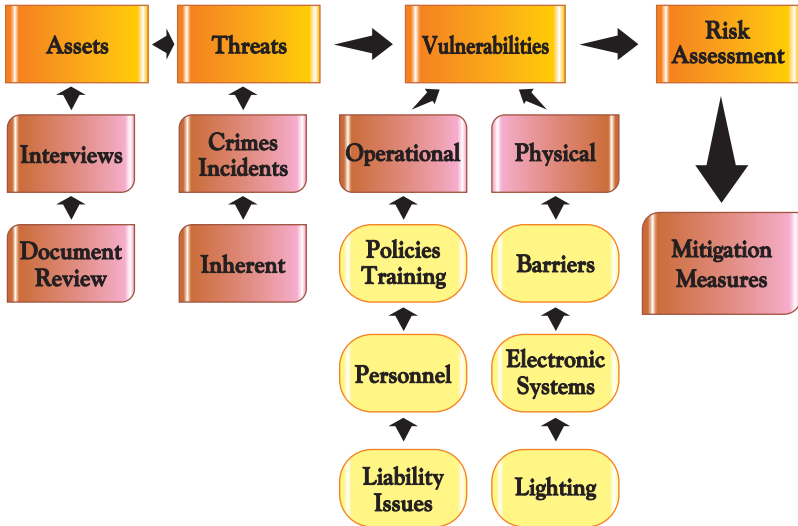
## Risk Register

It is an inventory list of all associated and relevant risks to the assets. It is also a locally-maintained analysis tool that feeds into the security risk analysis process.

### Sample

EXPOSURE	SOURCES	POSSIBLE IMPACT	ALLEVIATING FACTORS	AGGRAVATING FACTORS
Fraud in purchasing department	Computer database manipulation by lone or colluding employees.	Direct losses of N100million a year. Over-budgeting leading to skimming and further growth of fraud. Risk of fraud culture.	Stable employee/ employer relations. Database networked so remote inspection possible	Lack of direct supervision. Inadequate peer checking systems. Checks have never been undertaken.

## Security Risk Assessment Process



## Risk Mitigation

Risk mitigation is accomplished by decreasing the threat level by eliminating or intercepting the adversary before they attack, blocking opportunities through enhanced security, or reducing the consequences if an attack should occur.

Given a specific risk, there are five strategies available to security decision makers to mitigate it which are;

1. Avoidance
2. Reduction
3. Spreading
4. Transfer
5. Acceptance

*Key information*

*In reality, the goal of most security programs is to reduce risk.*

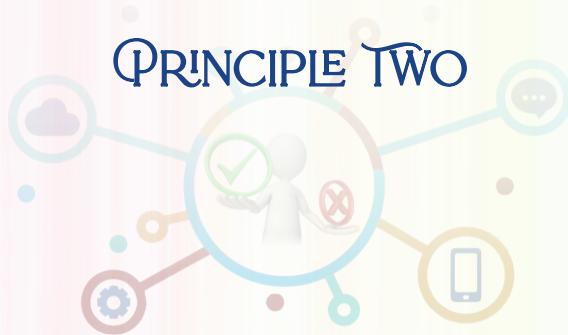
Meanwhile, in most cases it will not be possible to reduce risk to zero without stopping the operation, changing the way an activity is carried out or placing intolerable financial or obstructive burdens on the enterprise. Therefore, the objective of any risk management programme should be to reduce risk to “*as low as reasonably practicable*” or **ALARP**.

Using the ALARP concept, a common approach is to divide risks into three categories:

- Those adverse risks which are intolerable whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost;
- Those risks whose costs and benefits are taken into account and opportunities balanced against potential adverse consequences;
- Those risks which are negligible, or so small that no risk treatment measures are needed.

*Key information*

*Without question, the best strategy for mitigating risk is a combination of all three elements, decreasing threats, blocking opportunities and reducing consequences.*



## COST AND BENEFIT MUST BE BALANCED



### *Key information*

***Security is valuable, but comes at a cost.***

**O**ptimal security is the right balance of cost and the associated benefit which is a reduction or control of risks. Back in the day, this used to be called cost/benefit analysis, but it is being referred to as operational risk management in security. Operational risk: the risk of loss resulting from inadequate or failed

internal processes, people, and systems. While a cost-benefit analysis is specific to each enterprise, the methodology is the same. The methodology is a risk management model which ensures an understanding of the corporate assets, prioritization of value and current state of vulnerability based on design criteria.

Security may be capital intensive investment and a major deduction on the bottom line. As a fixed cost, the security budget has to compete with many other areas of the businesses or lifestyle that have an equally valid case for investment. Arguing in simplistic manner, FUD terms that *“without security there would be no business”* isn't perceived by many corporate entities or individuals as a sufficiently intelligent business case.

Meanwhile from a business perspective, security is usually about reducing losses (**operational risk management**), not profits making. One of the hardest tasks facing security professionals is to present the case for security using metrics to quantitatively (**data**) demonstrate the value of the security activity on the bottom line.

There are many ways in which metrics can be analyzed and demonstrated, but it is financial metrics (**return on investment**) that will be of greatest interest to your board of directors.

Sometimes security measures have to be in place to satisfy contractual, insurance or governmental

requirements, but for most enterprises it is a business decision, measured against the potential loss in the absence of measures.

It cannot be assumed that just because loss, or the potential for loss, exists, a business will always mitigate that loss potential to the extent possible.



*Key information*

*The objective of loss reduction is not to as low possible but instead to ALARP - as low as reasonably practicable by PROTECTING WHAT IS IMPORTANT ONLY.*

***Security is not free but should not to be expensive!***

Determining the most cost-effective solution to mitigate that asset varies from corporation to corporation based on the level of risk an organization will accept. Some enterprises are entirely risk-averse while others will accept some level of risk.

**The main part of the business case should be based on two elements:**

- a. The quantification of recoveries made or security incidents avoided during a given period.*
- b. The results of the security risk analysis (SRA) expressed in terms of quantified loss potential.*

***Formula;***

*Return on investment (ROI) = Recoveries Made + Avoided Loss as quantified by the SRA / Cost of Security Programme*

As a Chief Security Officer (CSO) or security manager with any organisation today should demand an executive personnel who is both a business leader and security practice and technology professional. Creating a world-class security program starts with building a team of experienced people who can adapt to the macro-level demands of the business they work within and still drive the organization's safety and security mission.

Security professionals are required to identify how to build security programs that mitigate exposure and vulnerability while continually delivering savings and efficiencies into the corporate enterprise. The ability to deliver an outstanding security program while watching the bottom line is as much art as science for today's CSO.

As security programs become more comprehensive and technically advanced, so do the expectations of companies who have a top security official in place. CSOs with technical backgrounds must also understand compliance, regulation, security, and risk beyond the data center. CSOs, whose primary experience is from a physical security, law enforcement or military background require an understanding of cyber risks and the threats they posed to their organization's overall assets.



*Key information*

*Physical security has evolved from a "cost center" to an "expense saver" due to the benefits associated with evaluating risk scenarios, costs and integrated solutions from a total cost of ownership standpoint.*

Security is about reasonable controls to manage the risk of loss.





**Good Security= Less Inconvenience + Less Cost**

**M**ost often, security is being perceived to be unnecessary obstacles, curtailments of freedoms - and an unnecessary cost which in turn makes security to be expensive.

A lot of people hesitate to install security systems or tools because they worry about inconveniencing their customers, their visitors or themselves. They worry that security tools will be too difficult to use and they'll make running a business more complicated than it already is. These fears leave them unprotected and vulnerable to

criminals.



*Key information*

***Security doesn't have to inconvenience people.***

Safety comes first but sometimes it may also slow you down.

Security systems and operations should be designed to be cost-effective, delivering value for money and simultaneously causing as little inconvenience to both the corporate operations and individuals or employees. From an employee's point of view, well trained and managed security personnel will cause less inconvenience and thus make security more acceptable.

A good example of an effective, cost-efficient but not burdensome, security measure is encryption on laptops. From a user's point of view encryption is transparent, causing no greater inconvenience than a regular password. From the enterprise's point of view it may represent the difference, if the laptop is lost, between the inconveniences of loss on the one hand and competitor advantage, embarrassment, or even a fine from a regulatory body on the other.

A business owner does not have to choose between secure and convenient. With the right tools and strategies, security can stay out of your way while still protecting your business when you need it. Rather than

consider it an inconvenience, it's important to look at physical security as a crime deterrent. The majority of criminals want to be in and out of a crime scene quickly. This means that they search for properties where there is little resistance. Installing security gates on your doors and windows will deter these criminals.

One example of this is security gates. For some people, the phrase “*security gates*” reminds them of large, permanent bars on doors and windows. They worry that these gates will make their property look “*like a jail*”. They're scared of chasing customers away with unsightly gates that make it difficult to see through the windows.

Security managers should always be cognizant that one of their primary objectives is to deliver the best possible security at the lowest possible expense and inconvenience to the mission of the enterprise. It's important to weigh any possible inconvenience that security tools could cause against the greater inconvenience of allowing criminals to rob your property.

Most importantly, security should be seen as a business enabler.



## **SECURITY MUST DEFER TO HUMAN FREEDOM**

**I**n the beginning, America invested in freedom, not the security of what its citizens already knew. And while both are vital to the success of a nation, freedom is the more fundamental, more enduring, and, therefore, more important. But after 9/11, security in America was taken to a new level with increased airport safety procedures, a stronger border control, and new security acts being passed.

Freedom and security need to be balanced, but freedom should not be jeopardized in order to obtain security.

Sometimes, we sacrifice freedom for security, and we need to do so.



Key information

*Living a life in security and freedom!*

Security measures need to find the delicate balance between creating optimum conditions for initiative to flourish and not being so restrictive as to stifle initiative. There must be trade off to ensure balance between freedom and security.

Security must also not violate privacy. There have been several documented cases where, for example, the use of covert cameras in situations where the person monitored might have a reasonable expectation of privacy (such as in a changing room or toilet) has led to prosecution of the person who deployed the camera.

Furthermore, when security measures become obstructive to the point that they hinder normal activities, people will surely find ways around them.

We need to feel inner happiness to be really secured and we cannot have inner happiness without freedom.

- *Freedom without Security is a probably short, chaotic and unsafe life.*
- *Security without Freedom is heinous.*

Can the two be achieved? Yes, when there is right the sense of security.



## SECURITY SHOULD ADD VALUE

**S**ome security managers or professionals cannot convince boards or clients on value(s) that security can provide, they just don't speak the language, and they turn them off even with egos.

Boards or clients think of ROIs and SWOT analyses, most security professionals don't.

Security is often seen as a cost center and not a revenue-producing entity. And security budget should depend upon the demonstrated added value of the assets

protection or security program to the organization.

Demonstrating business value can be much easier for enterprise units such as sales, production, procurement, even for IT. But for functions such as compliance, risk management or corporate security demonstrating value is far more challenging.

Security professionals usually fall for the temptation of thinking they are simply '**necessary**' somehow, part of the cost of doing business. This is a mistake. They are to help achieve business goals, top-line and bottom-line, as effectively as possible, with the least waste possible. And if nobody else is measuring their contribution, then they should be the ones to worry about how to do it best.

However, wherever possible security should add value. If security is seen as a discrete function that adds no value, it will be difficult to establish an integrated protection system using people, equipment and procedures.

**Key ways to add value are:**

1. Diversifying the role of the security manager to encompass other aspects of resilience, such as emergency management, crisis management, business continuity and due diligence.
2. Diversifying the roles of the security team to include health and safety, emergency and fire first response, and first aid.
3. Selecting security systems that offer multi-

functionality and enterprise-wide benefits in terms of cost savings.

4. Using technology as a force multiplier and less reliance on expensive manpower.
5. Using security measures only when there is no other crime prevention or business practice alternative to reduce opportunities or motivations for deviance and criminality.



*Key information*

It may be smarter to introduce procedures that address business expediencies, security and health and safety simultaneously.

Security shouldn't be seen as a cost center but *“a strategic investment in reduction of corporate risk, and a positive contribution to the realization of business value.”*

### 3 strategies to prove security's value

1. **Measure against risk:** Security about understanding the risk appetitive of the business and then building fences around it.
2. **Quantify security's role in business success:** Identify the contribution that security makes to the success of specific projects and initiatives, and then keep measuring it.
3. **Use metrics that matter:** Use of valuable



numbers, measure of resiliency and benchmarking with other organisations.

Good security knowledge needs to be accompanied by business skills and an understanding of business processes.

How can anyone influence the business with security advice if that person does not understand both business processes and security principles?

Summarily, security contributes to company or corporate profits by reducing or eliminating preventable losses, including those caused by criminal behaviour.



## **GOOD SECURITY IS THE EFFICIENT SUM OF ALL PRACTICABLE MEASURES**

**P**eople, Procedures and Equipment (PPE) make up the three basic ingredients/measures of a security system. It is important to employ these in the correct relationship (efficient combination and in accordance to the risk).

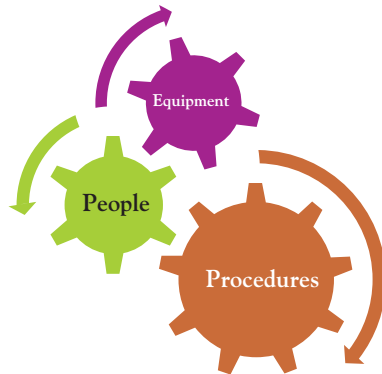
Generally speaking, procedures are the least expensive to implement but they require people's buy-in. Unreasonable procedures lead either to circumvention or undesirable obstacles to business processes, which, in

turn, lead to reduced profits. Security procedures and processes must be logical and systematic.

It could also be argued that the best system is that which employs the most acceptable combination of equipment, manpower and procedures.

Care should be taken to combine security measures in a way which is conducive to day-to-day operations, and which does not place security obstacles in the way of efficiency (and by implication profitability). All too easily, security measures can be employed that cause inconvenience.

The term “most efficient combination” relates not only to being efficient in relation to the risks, but also to cost. In many environments security manpower is often the least expensive initial investment, but it has an ongoing cost. In the West, conversely, security manpower is relatively expensive, and reliable electronic security systems can be purchased at relatively low cost.





*Key information*

***The Best Security System is that which employs the most efficient combination of Equipment, Manpower and Procedures. --- Integrated Security***

Therefore, a good security manager must possess both executive and technical competency because technology is the future of security now.



## DON'T BUILD IT ON; BUILD IT IN

**S**ecurity is actively avoided or hardly being forethought across the African continent as organisation or individual usually considers security as an afterthought for every establishment or development. It is a big challenge and dangerous practice especially in now digital world.

Lately, Africa's rapidly improving digital infrastructure and increasing internet accessibility have resulted in investors scrambling to tap into the world's last digital frontier. The current threat landscape means that

security can no longer be an afterthought for businesses, so it needs to be cooked into every part of an organisation from the start rather than added in after. It is cheaper and easier to build proper security in from the start.



*Key information*

***Physical security measures should be “built-in” at every development's design stage.***

The most efficient and cost-effective method of instituting security measures into any enterprise, facility, building or operation is through advance planning – by means of a thorough security risk analysis and continuous monitoring throughout the project or programme. Simply put, security would be a lot better if it is given just a smudge of forethought to vulnerabilities.

It is a rule of thumb that security measures that are designed in at the outset may cost as little as one third of those which are later superimposed on a ready-constructed facility. The downside is that until the facility is built and operations are underway, some risks may not be apparent. The solution is to construct a baseline level of security for all facilities, just as is the practice with domestic security and door/window hardware.

*Key information*

*Security should be an embedded full-stack solution, not an add-on; “Secure by design” needs to become the core approach to avoid security chaos in the not too distant future.*

Built-in security gives resilience and helps to build healthy security culture. A sustainable security culture is bigger than just a single event and when a security culture is sustainable, it transforms security from a one-time event into a lifecycle that generates security returns forever.

**“Built-in Security”** (infrastructure mindset) has four defining features;

1. It is deliberate and disruptive.
2. It is engaging and fun.
3. It is engaging and fun.
4. It provides a return on investment.

***Stop and think!***

***Can security stop all attacks?***



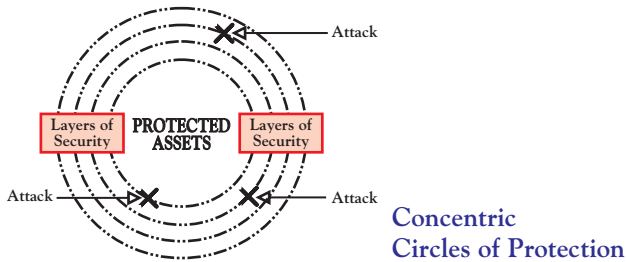
## **THAT WHICH PROTECTS MUST ITSELF BE PROTECTED**

**T**his could be referred to as layered security (onion skin approach) or defense in depth. The best security systems are those that are comprised layers that include different kinds of measures, designed to complicate the adversary path.

The desired objective is that the adversary will be deterred and the underlying assumption is that, vulnerabilities in one security layer will be compensated by the strengths of another.



Layered security arises from the desire to cover for the failings of each component by combining components into a single, comprehensive strategy, the whole of which is greater than the sum of its parts, focused on technology implementation with an artificial goal of securing the entire system against threats.



This concept involves the use of multiple “rings” or “layers” of security. The first layer is located at the boundary of the site, and additional layers are provided as you move inward through the building toward the high-value assets.

Rather than placing full reliance on a single layer of defense, these layers require an intruder to penetrate a series of layers to reach his goal. The more layers that exist between the outside world and a high-value asset, the better the security!

**Important Note:** *There must be an opportunity to detect, deter and delay an intruder at each boundary. This allows intruders attempting to penetrate the layer to be detected and intercepted with an appropriate security response.*

The Concentric Circles of Protection concept is similar to the “*multiple lines of defense*” strategy employed by many military planners

## Defense in depth

Originally coined in a military context, the term “**defense in depth**” refers to an even more comprehensive security strategy approach than layered security.



### *Key information*

*Layered security arises from the desire to cover for the failings of each component by combining components into a single, comprehensive strategy.*

Defense in depth, by contrast, arises from a philosophy that there is no real possibility of achieving total, complete security against threats by implementing any collection of security solutions. It widens attention to security scope and encourages flexible policy that responds well to new conditions, and ensures one is not blindsided by unexpected threats.

### *Stop and think!*

How many layers could be sufficient for effective

*Key information*

*“The best form of self-defense is not putting yourself in a position where you have to defend yourself”*

*— Martial Art*

protection?

Hence, now it is time to shift from **Defense-in-depth** to **Security-in-depth**.

Security in depth means simply adding another layer to the defense-in-depth philosophy. This layer will not provide additional security in terms of real-time detection, but it will reveal more insights in the overwhelming log data.

Attackers usually leave breadcrumbs before a major attack and by applying data analytics techniques, security teams can discover these hidden breadcrumbs to take appropriate action.

Summarily, the security-in-depth philosophy is about analyzing available and ingested data with a data science approach to reveal attackers' activities and intentions. It is also designed to determine whether existing layers of the defense-in-depth infrastructure are still working.

***Data-driven Security!***



## SECURITY SYSTEMS SHOULD CONTAIN AN ELEMENT OF SURPRISE



*Surprise produces fight or flight.*

**A** surprise is like a mini fight-or-flight moment in our brains. Many people are living a life of the same old same old. Do A, we get B. It is usually a “cause-and-effect” autopilot experience. When we experience a surprise, when we have a set of expectations and we get something else, our brain doesn't really know what to do with it. Surprise is about human cognition, perception and psychology.

Surprise often is described as a force multiplier, something that increases the effectiveness of one's forces in combat. Across cultures and history, military doctrines have encouraged soldiers to incorporate surprise, along with other force multipliers such as the use of cover or maneuver, into their military operations because they increase the prospects for success.

While deterrence is a key design objective of security systems, it may be unwise to reveal to potential adversaries the entire spectrum of surveillance, detection, delay and response measures in use, since the proficient criminal is usually able to make an accurate assessment of the effectiveness of visible security measures and how to overcome them. By using varied - and not obviously apparent - security measures along the adversary path, the action can be complicated by forcing the adversary to constantly change tactics and requiring different tools and methods to overcome each obstacle.

What a lot of people forget is that when a criminal is going to commit a crime they are going to be scared; they are breaking the law and can get arrested, beaten up or shot in the process. Criminals look for easy targets; they don't want problems as they are bad for business and most times they don't prepare for surprises.

Surprise destabilizes adversaries. A good security system requires element of surprise so as to possess

protection edge.



*Key information*

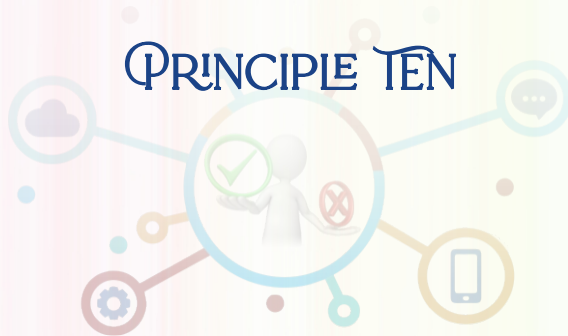
*Criminals look for people who are not paying attention to their surroundings, and then use the element of surprise to their advantage.*

***Stop and think!***

***Why do criminals mostly choose night to operate?***

***Surprise is attractive to the weaker party in a conflict because it allows it to contemplate decisive actions against a stronger adversary. -Element of Surprise***

There is nothing quite like the element of surprise when you want to get to the core of an issue. When one does not expect something to happen, there's no time to think about what his/her response should be.



## **THE FIRST BREACH OF SECURITY OCCURS WHEN TARGET EXISTENCE IS KNOWN**

**T**his means that the first breach of security formation or system occurs when the enemy becomes aware that the information worthy of targeting exists. If one uses metaphor of genie, it is at the point when the enemy knows about the information that the proverbial genie has been let out of the bottle and there is no way of returning it. At that juncture, defensive/offensive counter intelligence operations will come to play.



### Key information

**Intelligence is the product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of collected information which could be used for or against SECURITY.**

Intelligence is divided into strategic and operational intelligence. As intelligence is very critical for good security so also it is very important for the crime perpetrators.

**Counter-intelligence** is the exerted efforts made by the **intelligence** security formation to keep crime perpetrators away from gathering information against them.

Pretty simple: **“Intelligence”** is information collected to further your mission while **“Counter-intelligence” (CI)** is concerned with either catching those trying to gather intelligence otherwise disrupting the intelligence gathering process. CI may include planting **“fake”** intelligence to mislead the collectors

The emergence of the internet means that information about the nature of sensitive facilities is now much more accessible to any potential intruder undertaking research. Contractors, in particular, have a very bad habit of boasting about their clients on the internet, so procedures must be in place in Procurement for every contractor to sign a non-disclosure agreement. Care



should be taken about what finds its way onto the internet. Senior expatriate managers are often photographed and names posted on company website, or in online company magazines. When these executives are operating in, or visiting, high-risk countries this practice can expose them to greater danger. And with the use of easy-to-access online tools, home addresses and phone numbers can quickly be ascertained and in some cases families harassed and threatened.

Facilities that may be the target of activists, terrorists, or asset which possesses high-value theft targets may choose to adopt a low profile, with minimal overt branding. Corporate headquarters, too, are often better served by a small brass plaque at the main entrance rather than a large neon light promoting their logo.

Confidentiality is very key to good security practices. Every business/organization should have a written confidentiality policy (typically in its employee handbook) describing both the type of information considered confidential and the procedures employees must follow for protecting confidential information.

Under certain circumstances, information is only as good as the security measures used to protect it. Sometimes the best way to protect sensitive information or a proprietary secret is to limit the number of people who can actually possess it.

## Never trust, always verify

The Zero Trust approach uses the guiding principle of 'never trust, always verify'.



### *Key information*

*Zero-Trust security is the process of eliminating points of vulnerability by limiting access to vital information, as well as adopting extensive identity verification.*

### *Stop and think!*

How much about you is out there?

*Keep low profile to stay safe.*



## THE “NEED TO KNOW” RULE

*Need to know means the user has a legitimate reason to access something.*

**A** criterion used in security procedures that requires the custodians of classified information to establish prior to disclosure who should know, to what extent and why. Least Privilege can then be implemented to limit that access and limit what the user can do with that something. The principle of least privilege (POLP), also known as the “principle of least authority” is a security concept

based upon limiting access to the minimum necessary for an action to be performed.



*Key information*

*It is a general knowledge that the business growth depends on sharing of information and know-how.*

Enterprises that are unnecessarily keeping away operational information generally do not create the conditions in which business will flourish. Those that do share information and know-how, and which encourage initiative are usually the more successful.

However, access to some information should be restricted to a “*need-to-know*” basis so as to avoid or prevent sabotage.

Obviously, in order to implement a need-to-know policy, sensitive information must be correctly identified and those who need access determined depending on certain **factors**. Take for instance, the seniority of an employee in an organisation is not necessarily an indicator of need-to-know privileges. Even if one has all the necessary security clearances to access certain information, this doesn't confer on that person an automatic right to access all sensitive information of that level of classification.

As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without

inconveniencing legitimate access. Need-to-know also aims to discourage "**browsing**" of sensitive material by limiting physical and IT access to the smallest possible number of people, so need-to-know protocols should be replicated across the intranet.



#### Key information

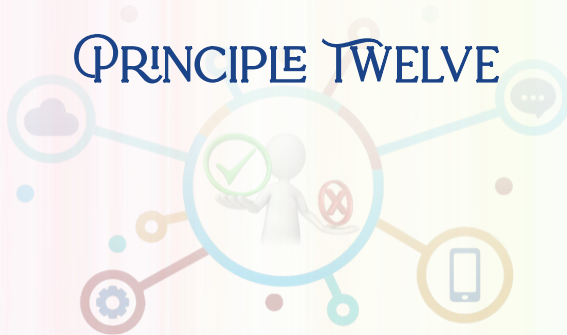
**Failure to adopt “*need-to-know principle*” has turned so many domestic workers to killers because of too much information about their principals at their disposal.**

#### ***Stop and think!***

What does the term "*the more you look, the less you see*" mean? And does it apply to "*need-to-know*"?

### **Security through Obscurity**

The "*security through obscurity*" strategy is based on the theory that if you keep a low profile, attackers will "*pass you by.*"



## THE “NEED TO GO” RULE

**A**ccess management is a core security management process for managing who (or what) can go where and when.

There are two kinds of access management:

- Physical access management
- Logical (IT systems) access management

Access management is often regarded as the most important security component for the provision of effective physical security, and some form of access

control should be applied at every facility. Access control systems make life easier for your employees, save you money and keep your workplace secure.



#### Key information

*Access management is only one aspect of the overall security arrangements of a facility; it should be designed to complement other measures which are in place.*

Importantly, access management is based on the presumption that the boundary of the space to be protected is secure and that control is provided at every point of entry/exit. The number of entrances and exits should be as low as possible, consistent with operational requirements.

In some facilities/premises, almost all people have access to every areas/locations. While we need to allow freedoms for initiative to thrive and the business to flourish, there should be an effective, compartmentalized access management programme in place, with appropriate access privileges, based on a combination of;

- Identity
- Work group or work area
- Role or management level

This makes sense not only from the security perspective,

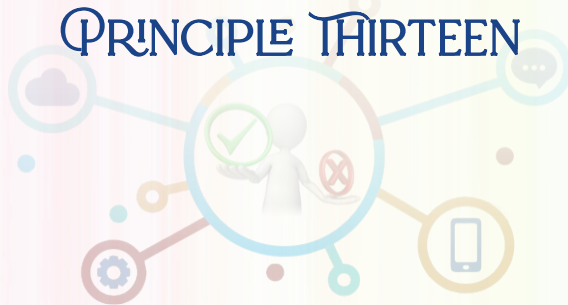
but also avoids exposing staff to unnecessary health and safety hazards. Procedures should be in place to govern where a particular member of staff may and may not go. Other reasons for doing this may include to;

- Reduce exposure to internal theft
- Make it easier to investigate theft
- **Help achieve “need-to-know” rule**

Also, the need-to-go principle can be replicated across the intranet system (IT security) in relation to network browsing permissions. Access levels must be created.

In theory, access management is relatively easy to achieve. The facility is enclosed within a secure perimeter, the inside is zoned into critical and less critical areas, cards are issued to all those seeking access and the system is configured to allow access only to those who have a need to be there. In practice, this may not be so easy to execute.





**ANY SECURITY SYSTEM IS ONLY AS GOOD  
AS ITS WEAKEST POINT**



*Key information*

*All systems have weakest link, and there several strategies for securing systems despite their vulnerabilities.*

**T**here are a number of ways of looking at this principle.

*“A chain is no stronger than the weakest link.”* It's an

axiom we've understood since childhood. No matter how strong the strongest links of a chain are, no matter how many strong links there are in it, a chain will break at its weakest link. Improve the strength of the weakest link and you improve the strength of the chain. Whatever you do to any other link of the chain won't make it stronger. A lot of security is like this. If your house has two doors, the security of the house is the security of the weaker one.

In the onion skin approach to security the idea is to create multiple layers of different types of security in order to complicate the adversary's path and to force him/her to have to employ multiple tactics and tools.

In short, the idea is an obvious one: that any single defense may be flawed, and the most certain way to find the flaws is to be compromised by an attack -- so a series of different defenses should each be used to cover the gaps in the others' protective capabilities. Where single-layer security systems are used (and this is not advised) there may be circumstances where a single weak point in that layer will compromise the entire system, rendering it ineffective.

If you're trying to protect a head of state in his office, home, and car, and while he's in public, his overall safety level is no higher than his safety level in the most insecure of those locations. Smart attackers are going to attack a system at the weakest countermeasure they can

find, and that's what a security system has to take into account.

Just as security is subjective, so is the weakest link. If you think you've found the weakest link in a system, think again.



*Key information*

***Finding the weakest link is hard enough and securing it may not be worth the trade-offs.***

More often than not, we improve security haphazardly, recognizing a problem and fixing it in isolation—often without looking at the whole system, without identifying whether it is the weakest link.

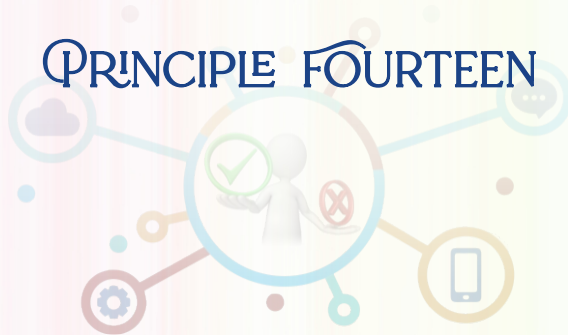
Your attack had two phases: create a weak link and then exploit it. Finding the weakest link is hard enough and securing it may not be worth the trade-offs.

- They ignore security policies and procedures at will easily – complacency.
- They can be coerced, blackmailed and socially engineered to compromise.



*Key information*

***Humans are often considered the “weakest link” in the security chain.***



## **THERE IS NO SUCH THING AS AN IMPENETRABLE BARRIER**

**I**t is impossible to build a barrier that cannot be compromised. If enough time, money, personnel, planning and imagination are used, any structural barrier can be penetrated. There two kinds of barrier; Natural and Artificial.

### **Types of Barriers**

1. Human
2. Animal
3. Natural

4. Energy/Electrical/Electronic
5. Structural

### 3 Lines of Defense

- **1st:** Perimeter Barrier
- **2nd:** Building Exterior
- **3rd:** Interior Controls

The purpose of a barrier is to prevent the penetration of an area by intruders.

However, as most barriers can be defeated with sufficient time and resources, then the purpose of a barrier is to delay the progress of the intrusion sufficiently for a response team to intercede and apprehend the intruders. Barriers are used for the protection or control of a diversity of assets including people, physical assets, sensitive data and information, and other materials.



#### *Key information*

***Security relies on a combination of manpower, procedures and mechanical defenses, and all have inherent weaknesses.***

Therefore, security professionals should view their defenses in terms of delays, rather than preventive measures. It is axiomatic that the more ways in which an asset can be compromised, the more vulnerable it is to theft, destruction, damage, harm, compromise or

denial.

**Deterrence, detection, delays and disruption (4-D's)** are the core building blocks of any security system design.

**Deterrence** is achieved by implementing measures that are perceived by potential adversaries as undesirable to attempt to defeat (cost, time, difficulty, surveillability etc.). Deterrence can be very helpful in discouraging attacks by casual adversaries, who may be displaced onto a less well protected target. However, deterrence is ineffective against a determined adversary who is set on specifically attacking you.

**Detection** of an adversary at early stage is essential. Early detection at the site perimeter increases the available response force time after detection. Adversary paths (typical routes taken by the adversary to reach an asset) should be anticipated, and detection elements deployed along that path with specific consideration given to how the chosen technology works in relation to the direction of movement. From a cost and business interruption perspective, detection is better when it takes place before an undesirable event rather than after.

**Delay** provides time for detection to take place. The terms delay and barrier are often used interchangeably, but they are not synonyms as the latter may sometimes infer an ability to prevent an adversary action. A barrier is a natural or manufactured obstacle to the movement

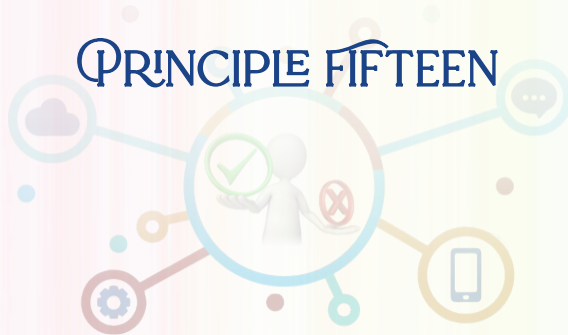
of persons, animals, vehicles or materials. It defines physical limits to and delays or prevents penetration of an area.

There are four main ways to defeat a barrier, summed up by the acronym **FADS: Force, Accident, Deceit and Stealth**. Some adversarial actions favour one type of attack over another, or may use a combination of approaches. Security systems should be designed to address all four approaches.

Disruption is a measure of the effectiveness of response in neutralizing the adversary and ideally preventing the undesirable event. Disruption is a combination of assessment, response and deployment, and neutralization. And for response to be effective, it must be completed before action has been completed and ideally before the penetration of the barrier has taken place.

### *Stop and think!*

It is not possible to construct a barrier that cannot be compromised. Any structural barrier can be penetrated if sufficient time, finance, personnel, planning, and imagination are applied to the assignment.



## **GOOD SECURITY SYSTEM IS THAT WHICH PROVIDES THE EARLIEST DETECTION**

**T**he best security system is that which provides the earliest detection, and strong delays can significantly assist in assuring that detection takes place, and that there is sufficient time to detect it effectively.

Detection is more than just sensing adversary action. For effective interdiction the information communicated to the response force should include details of at least the adversary:



- Strength
- Nature and sophistication
- Weapons
- Direction of travel
- Indication of the intended adversary action and target

This is why detection should always be augmented by assessment. The most common form of assessment is video surveillance (CCTV).

The quantitative measurement for detection systems is probability of detection. A security system with detection reliability of 0.95 (95%) under most normal circumstances is reasonable for an intrusion detection system. When deterrence, detection, delays and disruption are carefully configured in order to address external adversary intrusion this principle is relatively easy to implement, and requires little specialist skill.

A factor that should be considered in planning barrier protection is the prevention of surreptitious entry. If an intruder is forced to leave evidence of a penetration, prompt action can be taken to assess the damage, and plans made to neutralize the effects of the entry. Putting in place procedures to detect product diversion, or the insertion of a mole into the workforce requires a more sophisticated protection approach, undertaken in close collaboration with the business.

Essential detective elements include, but are not limited to:

- Close liaison with IT to detect unusual workstation or laptop activity on the part of employees. Establishing an outsourced telephone hotline for staff and contractors to report their concerns. Pre-employment screening.
- Covert surveillance.
- A culture where staffs really do believe that security is everybody's responsibility.
- Automated red flag software for scanning financial data.

More importantly, the physical protection plan should be designed so that if an intruder does succeed in gaining entry, some evidence of that fact will be left.

The adversary task time is the time taken by an adversary to achieve his/her objective.

## Crime Scenarios

**Theft:** This usually comprises entry into a specific area, acquisition of the target, and successful withdrawal from the area with the target in hand.

**Sabotage and Terrorism:** The adversary task time is considerably shorter since the objective is only to enter the area and commit the act of sabotage – the task is considered complete when the adversary reaches the

target and carries out the action.

The main reason for placing alarm systems as far as reasonably possible from the target is to increase the amount of time available to the security response team to reach the intrusion site and intercept the intruder. It should however be remembered that in some instances, placing the intruder detection system too far away will greatly increase costs and in some instances make it more difficult for the response team to locate the intruder, as, once detected, he/she is likely to speed up their action.

### *Stop and think!*

Can security threats be detected before they arrive?



#### *Key information*

***Protection by detection and elimination:*** *The capacity of any protection system to protect itself from criminal attack implies an improved mechanism for timely detection of a threat from the crime build-up.*

### **Threat Detection and Response –TDR**

It is a methodology that enables security operatives or systems to detect attacks and neutralize them before they cause disruption or become a breach.

## The TDR Framework

The framework is based on the military concept known as the OODA loop: Observe Orient, Decide and Act by enabling threat hunters and analysts to work in a consistent, structured way and ensure nothing is overlooked.

- **Observe:** what you see or notice (data/signal)
- **Orient:** what is the context, the behaviour, how does it map against known attack tactics, techniques, and procedures?
- **Decide:** is it malicious, suspicious, or benign?
- **Act:** mitigate, neutralize and re-enter the loop.

There are five key components of TDR that underpin the various stages of the framework;

1. Prevention
2. Collection of security events, alerts and detections
3. Prioritization of the signals that matter
4. Investigation
5. Action



## **TIME OF PENETRATION MUST BE GREATER THAN TIME OF DETECTION PLUS TIME OF RESPONSE**

**E**very second counts when it comes to incident response. With proper staffing (people), a streamlined procedure and the right tools (equipment) in place, responding to threats can be a far less daunting task. The severity of security breaches varies, but since damage done directly correlates to the time a malicious actor has access to the targets, it's paramount that all threats are discovered and remediated as quickly as possible.

The four elements of intrusion detection design (deterrence, detection, delays, and disruption) should be configured in accordance with the statement:

*Time of Penetration must be greater than Time of Detection plus Time of Response, abbreviated to  $T_p > T_d + T_r$ .*

- **$T_p$  = time of penetration**
- **$T_d$  = time of detection**
- **$T_r$  = time of response**

In order to satisfy this equation any one, or all, of the component following elements may be influenced;

- Increasing time of penetration
- Improving time of detection
- Improving time of response

## **Application**

### **1. Increasing time of penetration**

- Use of penetration-resistant fence or using two layers of chain link with coiled razor wire infill. Height of fence to 2.4m with additional 0.6m of coiled razor wire in V-shaped overhangs.
- Fence fabric embedded into concrete base.
- Patrolling guards or guard dogs

### **2. Improving time of detection**

- PIDS detection zone to extend beyond perimeter.
- CCTV field of view to extend beyond

perimeter.

- Patrolling and Improving surveillability.
- CCTV linked to PIDS for immediate assessment.
- Officer immediately available for assessment.

### 3. Improving time of response

- Relocation of after-hours guard post nearer to vulnerable areas.
- Quick reaction force.
- Patrolling and dogs.
- Appropriate response transport.



#### Key information

It is important to note that the adversary task time in relation to theft can be defined as *“the time to reach the target and escape after successful completion of the action”*.

This is, however, not the case if the adversary objective is sabotage or violence, when the adversary task time is usually *“the time it takes the adversary to reach the target”*. Irrespective of escape, once the adversary reaches the target the action element of the adversary task is usually complete.

**Stop and think!**

## **What is incident response?**

Incident response is a procedure that enables companies to detect, prioritize, and prevent security incidents. Incident response processes alert organizations about major security incidents, enable them to respond quickly and stop the attack. Quick response reduces damage and prevents further attacks or similar incidents.

### **Critical Incident Response Time (CIRT)**

A well-defined incident response plan should include;

- Detailed information about each phase of an attack.
- The six critical phases of incident response are preparation, identification, containment, removal, recovery, and learning from mistakes.

In addition, you need to test your plan to ensure your employees are updated about the latest security threats and standards. This can be the difference between a secured and vulnerable organization.





## THE STRONGEST PHYSICAL BARRIER SHOULD BE THAT WHICH IS CLOSEST TO THE TARGET

The "*defense-in-depth*" principle ensures that concentric layers of barriers protect the assets of an organization, and that only authorized people have access to the assets.

However, access can only be gained to the assets by crossing the barriers in the **DiD strategy**. The emphasis on design and use deviates from the target-hardening approach to crime prevention.

## Target Hardening

Traditional target hardening focuses predominantly on denying access to a crime target through physical or artificial barrier techniques such as walls, fences, gates, locks, grilles, and the like. Target hardening often leads to constraints on use, access, and enjoyment of the hardened environment.

## Design Questions

- How well does the physical design support the intended function?
- How well does the physical design support the definition of the desired or accepted behaviors?
- Does the physical design conflict with or impede the productive use of the space or the proper functioning of the intended human activity?
- Is there confusion or conflict in terms of the manner in which the physical design is intended to control behavior?

Target hardening can be categorized by the type of attack they oppose;

- Against forced entry
- Against destruction
- Against bomb
- Against toxins and air-borne agents
- Against violence

- Against all of the above

Moreover, the traditional approach tends to overlook opportunities for natural access control and surveillance. The term natural refers to deriving access control and surveillance results as a by-product of the normal and routine use of the environment. It is possible to adapt normal and natural uses of the environment to accomplish the effects of artificial or mechanical hardening and surveillance.

Nevertheless, Crime Prevention Through Environmental Design (CPTED) employs pure target-hardening strategies, either to test their effectiveness compared with natural strategies or when they appear to be justified as not unduly impairing the effective use of the environment.

The three CPTED strategies of territorial reinforcement, natural access control, and natural surveillance are inherent in the Three-D concept.

1. Does the space clearly belong to someone or some group? Is the intended use clearly defined?
2. Does the physical design match the intended use?
3. Does the design provide the means for normal users to naturally control the activities, to control access, and to provide surveillance?

## **Practical Implementation**

Relating back to the concept of layered security, the strength of outer (perimeter) defenses is often overestimated. A 2.4m chain link fence with razor wire has a delay value of just seconds, as do some doors and windows. Moreover, a perimeter is a very large area to protect from a cost perspective. Much better security can be achieved by concentrating valuables in one central place and securing them in a strong room or safe. It is important, also, not to overestimate the delay value of safes. Against a very determined intruder, with appropriate tools, many safes can be defeated in under 1 hour.

The same applies with residence security. The normal physical security of executives' residences may be sufficient to delay a burglar, but it will not usually be sufficient to hold back somebody who is determined to do harm to the principal or his family. In cases where the risk profile is high, consideration should be given to the provision of a hardened safe refuge, often a ground-floor bedroom specially strengthened for this purpose.

If measures are evaluated in collaboration with line management (and not as a separate security management activity) it will increase awareness and help ensure that regular employees contribute knowledge about the strengths and potential vulnerabilities of the security measures in place when compared against the assessed risks.



## THINKING LIKE A CRIMINAL IS GOOD FOR SECURITY DESIGN

### **A dangerous creative inspiration!**

**A** criminal's' desperation is the biggest variable to understanding the criminal mind.

When planning an attack, criminals study their target victims looking for the weakest links. In planning their attacks and seeking their victims, criminals look for the easiest access point, whether through inadequate

baseline measures, lax security policies and/or exploitable human compromise.



*Key information*

***Focusing too much on protecting only the critical assets might leave gaps in security for criminals who are seeking other valuable assets.***

The hackneyed expression, “*One man's trash is another man's treasure,*” serves as a reminder that what the enterprise or individual values is often different from what a criminal values.

The big idea is that people are very specifically and deliberately in committing crimes. And the intent of those criminal attacks, however, is not always the most valuable (the crown jewels). In order to create crime deterrence and prevention, one needs to think like the bad guys.

Thinking like a criminal helps to take an inside-out approach to vulnerability management. Threats change and evolve. It's valuable because no one has infinite resources, so you have to focus on the most probable and impactful threats.



*Key information*

***Think like a criminal to beat them at their own game but the problem is: the majority of people detest the idea.***

It may be great to have some of the energy that is a characteristic of a criminal but their thinking is often based upon fear - a widespread, persistent and intense fear. Like the fear of being caught. Criminals also often experience themselves as being nothing, a state of worthlessness and hopelessness.

Moreover, criminals tend to think of particular objects and events rather than abstract concepts. But thinking like a criminal may give you a unique perspective upon the world.

### **Stop and think!**

Put yourself in a **criminal's** shoes and **think** how you would rob or kidnap yourself. How would you break into your home or office?

***Make a list of your vulnerabilities. –Security Mindset***

Security requires a particular mindset. Security professionals, at least the good ones see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to compromise the voting system.

***They just can't help it.***



### **SECURITY-INFORMED SAFETY: IF IT'S NOT SECURE, IT'S NOT SAFE**

**T**raditionally, safety and security are often treated as separate disciplines, but this position is increasingly becoming untenable and stakeholders are beginning to argue that if it's not secure, it's not safe. The idea of combining safety and security is not new but neither is it straightforward. Need resilience as well as safety!



In principle, achieving interworking between safety and security should be straightforward. Both are sophisticated engineering cultures that emphasize the need for good process, the importance of risk analysis and the need for assurance and justification. When dealing with safety and security, terminology is important as the different communities can use the same terms to mean different concepts, and have different terms for the same concepts. In this short article we clarify the difference by noting that;

- Safety is concerned with protecting the environment from the system whereas
- Security is concerned with protecting the system from the environment.

However, these similarities are superficial and in practice there are significant challenges, as experience with large-scale systems has shown. Safety is concerned with protecting the environment from the system whereas security is concerned with protecting the system from the environment. For a system to be safe, it also has to be secure. Otherwise, a safety critical system – one that can harm or injure people – could provide attackers with a potential mechanism for causing widespread damage or panic, and it is credible that such systems could become the target of malicious actions.

Security and safety can both be viewed as kinds of dependability (in the sense that each is concerned with mitigating the effects of a particular kind of failure) and

the two disciplines uses similar techniques to identify potential failure modes and assess their impact on the overall system. Thus, there is considerable overlap between safety and security methods, although the focus is different and in some cases safety and security requirements can be in conflict. It is important for a system to remain safe and secure despite changes to the environment, in other words, to be resilient to change.

Risk assessment is a fundamental step in safety and security analysis, but the underlying threat model is different. There is a need for a unified methodology for assessing the threats to the safety and security of a system.

Security considerations can have a significant impact on a safety case. For example, there needs to be an impact analysis of the response to security threats and discovery of new vulnerabilities and reduction in the strength of protection mechanism. This suggests a greater emphasis on resilience of the design. It is also necessary to consider the potential for attack during a safety incident and the opportunity this might provide for malicious activity.

A fail-safe state may not be as safe as previously thought if the system is under attack and the assumption that any security attack on a control system could only, at worst, cause a fail-safe state to be reached is in general not true. Moreover, assumptions about the capabilities

and state of society may change; for example, consider managing a safety incident during a major security incident.

There are a variety of initiatives to integrate security into hazard analyses such as using security (or cyber) informed Hazard and Operability (Hazop) studies to assess the architectures of industrial systems. Another area where there is common ground between security and safety is in static analysis of code. Both security and safety perspectives are needed to assess the likelihood of vulnerabilities being exploited and the effectiveness and consequences of their mitigations.

## **Security-informed hazard analysis**

One of the key topics in PAS 11281 is the impact of security on risk assessment covering the whole life cycle of the vehicle. The PAS states that security concerns could have an impact on:

- The system boundaries
- What systems could potentially affect safety
- The stakeholders involved
- The validity of design safety assumptions.

Therefore, care must be taken during the analysis to account for security concerns as well as safety.

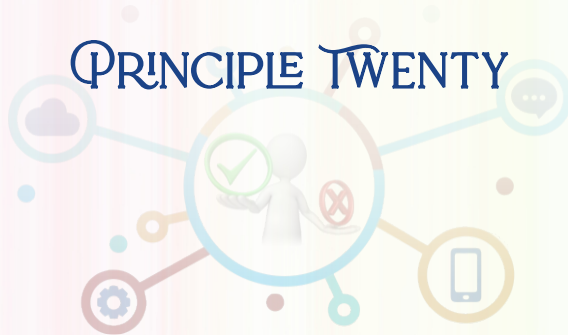
### **7-step security-informed safety risk assessment**

**Step 1:** Establish system context and scope of

- assessment.
- Step 2:** Configure risk assessment.
- Step 3:** Analyze policy interactions.
- Step 4:** Preliminary risk analysis
- Step 5:** Identify specific attack scenarios
- Step 6:** Focused risk analysis
- Step 7:** Finalize risk assessment

The deployment of autonomous technologies may follow an innovation cycle that first focuses on functionality and seeks to progressively add additional assurance and security. This will make the development of the assurance and safety cases and associated security and safety risk assessments particularly challenging.

*Don't pay twice for assurance!*



## SECURITY IS NOT JUST A PRODUCT BUT A PROCESS

In today's connected world, security is a constant concern and the rules for security are changing daily. Avoiding threats is black and white: either you avoid the threat, or you don't.



### *Key information*

*Avoiding risk is continuous: there is some amount of risk you can accept, and some amount you can't. Security processes are how you avoid risk.*

Security processes are not a replacement for products. Rather, they're a way of using security products effectively. They're a way to mitigate the risks.

The challenge is that no single security solution is as good as it claims to be. You can't buy a blinking box or a piece of software and be secure. This is because without configuration, no one product can solve all your organization's unique security needs, and because secure isn't a finish line or a checklist.



#### Key information

*Today's threat landscape is evolving rapidly, and a static security posture is simply insufficient. We must approach security as a process, a mindset, a way to view the world. Effective security requires the integration of people, processes, and technology into the bigger picture of business strategy, value, and risk.*

Ultimately the integrity and security of your technical environment will reflect the maturity of the people and processes that manage it, not the other way around.

In fact, most security programs rely on many processes to meet their objectives. Instead of "*a process*", monolithic and singular, security is actually a portfolio of organizational processes that can be as complex and specialized as the equipment running within the infrastructure.

Some of these processes complement one another. Others compete and conflict. Most demand unique skills and knowledge, from threat intelligence to assessments and audits to incident response. And each of these processes is an individualized enterprise asset that, like other resources, must be made to interoperate efficiently and effectively within the whole.

Along with process and technology, security programs need strategic leadership, skilled performance, and effective asset orchestration. An organisation can have the best security technology in the world, the most well-designed security processes and best practices in the industry. But these resources won't manage themselves. If security leadership can't proficiently keep those disparate, specialized assets in balanced operation, sooner or later everything comes crashing back to the ground.



*Key information*

***Security is an attitude!***

## REFERENCES

ScienceDirect Journal & Books, <https://www.sciencedirect.com>

Halkyn Consulting Security & Risk Management, <https://www.halkynconsulting.co.uk>

Real Time Networks -Physical Security 101, <https://www.realtimenetworks.com>

The International Security Management Institute, ISMI UK, [www.ISMI.org.uk](http://www.ISMI.org.uk)

National Training Center (2006), [www.nationaltrainingcenter.net](http://www.nationaltrainingcenter.net)

Marko Cabric (2015), Corporate Security Management, Challenges, Risks and Strategies

Parker D B (1981). Computer Security Management, Prentice Hall

Protective Security Policy Framework, <https://www.protectivesecurity.gov.au>

Security Culture and Strategy, <https://www.csoonline.com>

Ramirez, J. Martin, Biziewski, Jerzy (Eds.) (2020), A shift in the security paradigm

Health and Safety Executive, [www.hse.gov.uk/simple-health-safety](http://www.hse.gov.uk/simple-health-safety)

Robin Bloomfield, Centre for Software Reliability City University London