“One of the most important ingredients in effectively managing an emergency event is communications.

“One of the most important ingredients in effectively managing an emergency event is communications.

Investigation -Objectivity, Thorowness, relevance, Accuracy, Timeliness (Attributes/qualities)

Five resources of Investigation - People, information, credibility, physical assets , financial assets

Four Phases of investigative life cycle - Initiation of investigation, The investigation itself, Reporting , use of the information

Three tools (3 Is) - Information, Instrumentation, interrogation,

Three Important Force Multipliers in Investigation-Liaison, Online information sources, Intelligence Information

The five basic steps of report writing- Gather the facts, Record the fact immediately, organise the facts, write the report, evaluate, and edit the report if necessary

Key Qualities of a successful security Manager- • Patience • Wisdom • Virtue • Empathy • Kindness • Trust • Knowledge • Self-control

To meet its objectives and implement its strategy, a business must pay attention to its primary resource: its people.

The Human Resource (HR) department is one of a company’s most valuable departments

The most visible component of the HR department is staffing

The direct requirements are those that the candidate must meet to understand and function in the position. The indirect requirements are skills that will increase the candidate’s likelihood of success.

After employees, corporate knowledge is the second most valuable resource, and supporting knowledge management supports the organizational strategy. A central knowledge management system collects, distributes, and publicizes corporate data in a searchable, accessible format.

Of course, a central knowledge management system may also create a security vulnerability. Because the information could be accessed and exploited by competitors or other outsiders, it is essential to keep the information system secure.

As members of their employers' management teams, security managers must understand more than security—they must also know business and finance.

A financial strategy is management's financial approach to determining the expected returns of its investments (including its departments and operations) and estimating and managing the relevant risks.

In establishing a financial strategy, the first step is to identify expected margins, or the profit that businesses generally make

Realistically a company has two options if it wishes to improve margins. It can reduce costs or increase the price of its product or service

The question is how to fund growth. Growth can be funded from internal cash reserves or through commercial financing and investors.

Three financial reports or statements have become accepted as standard: the income statement, balance sheet, and statement of cash flows

Financial statements are created in accordance with generally accepted accounting principles (GAAP). These principles vary somewhat from country to country. Many countries are converging on the International Financial Reporting Standards (IFRS

The income statement outlines the organization's profitability but does not provide a picture of the organization's overall financial health. The balance sheet aids in that assessment.

The balance sheet summarizes an organization's investing and financing. The report's underlying equation is as follows: assets = liabilities + shareholder equity

The primary limitation is that it does not directly consider changes in market conditions.

In the United States, financial frauds involving Enron and WorldCom led to the Sarbanes Oxley Act (SOX), officially known as the Public Company Accounting Reform and Investor Protection Act of 2002.
A budget is a process for planning where money is to be allocated for the year. It is a financial tool that estimates costs and revenue and provides a variance warning mechanism and fiscal uniformity for the company.

A standard is a set of criteria, guidelines, and best practices that can be used to enhance the quality and reliability of products, services, or processes.

Standards are of nine main types: basic, product, design, process, specification, code, management systems, conformity assessment, and personnel certification

In the security arena, one often speaks of protecting three types of assets: people, property, and information. The larger view of assets protection, however, also considers intangible assets, such as an organization's reputation, relationships, and creditworthiness.

Of particular interest today is convergence, which is the "integration of traditional and information [systems] security functions" (ASIS International, 2005)

five forces that are shaping the practice of assets protection: technology and touch globalization in business standards and regulation convergence of security solutions homeland security and the international security environment

Modern management is now more interested in preventing losses than in trying to buy insurance to cover every possible risk.

Peril has been defined as "the cause of a possible loss."2 - term Used in Insurance

direct loss, such as the physical loss of or damage to the object concerned

loss of use, such as the reduction of net income due to loss of use of the damaged or destroyed object

extra-expense losses, such as the costs of defending a liability suit and paying judgment or hospital and medical expenses following a personal accident

The solution to this problem is usually called "tail cover"—retrospective coverage for events that occurred during a prior policy period but are raised during the tail period. To change carriers, it is normally necessary to purchase tail cover from the prior carrier.

Coverage - Fidelity coverage is written to protect the employer from the dishonesty of employees

Coverage - Surety coverage is intended to guarantee the credit or performance of some obligation by an individual.

ROI = AL+R/CSP Avoided Loss + Recoveries made/Cost of security Program (Personnel Expenses, Administrative expenses, Capital expenses)

The term “security metrics” refers to security-related measurements.

WAECUP (Waste, Accidents, Error, Crime, Unethical Practices) can be used as a blueprint for developing security objectives.

SWOT (Strengths, Weaknesses, Opportunities, and Threats) Analysis is a model for analysing proposed organizational projects. The concept is to analyse an issue or proposal from each of the four points of view, thereby giving security management a profile of potential issues to deal with. A goal of risk analysis is the recognition of threats as they relate to company operations.

The STEP (Social, Technological, Environmental, and Political) Model points out potential sources of threats. The security manager can then conduct an analysis to determine whether such threats are likely and where they could come from

In the retail industry, up to 70 percent of losses are perpetrated by employees,

Employees steal more than food and cash—they steal time.

Time, finished goods, supplies, scrap and waste, and intellectual property are the assets most often stolen.

Lack of supervision and lack of effective processes are the primary contributors to employee theft and fraud.

Secretive relationships, missing documents, indicators of substance abuse, and irregular hours of operation or building entry are clues that employee theft or fraud may be occurring.

Although workplace theft first received scholarly attention in the mid-19th century, academia largely ignored the subject until the early 1980s

John Clark and Richard Hollinger (1982), researchers from the University of Minnesota Department of Sociology, published the results of their extensive three-year study on employee theft.

They defined employee theft as “the unauthorized taking, control, or transfer of money and/or property of the formal work organization that is perpetrated by an employee during the course of occupational activity.”

Clark and Hollinger found it difficult to separate theft from other forms of deviance. Their study also examined production deviance, such as unauthorized or extended coffee and lunch breaks, inappropriate use of sick time, punching timecards for other employees, and arrive late or leaving early. Each of those acts, by today's standards, constitutes theft of time.

The four characteristic principles involved in internal thefts scams include diversion, conversion, disguise, and divergence.

Embezzlement involves the fraudulent appropriation of property by a person to whom it is entrusted, which can involve material things such as art, property, and product, not just cash. Defalcation more specifically deals with the misappropriation of trust funds or money held in a fiduciary capacity

Two prominent explanations of white-collar crime are Edwin Sutherland's differential association theory and Donald Cressey's non-shareable need theory.

In the United States, the Sarbanes-Oxley Act (formally known as the Public Company Accounting Reform and Investor Protection Act of 2002) became law on July 30, 2002

The growth of private police is not a reflection of poor public policing.

The work of public and private police should be viewed as a division of labour.

When the first police department was organized by Sir Robert Peel in London in 1829,

This assertion was even reflected in one of Peel's guiding principles: the people are the police; the police are the people

If a crime is observed, the security officer should gather information about the criminal and the crime and then immediately report such to the public police. This is deemed as being the eyes and ears of the police

Over time, a more defined crime control system was established. This system, known as "watch and ward," was administered by "shire reeves," who were appointed by the king

Both the shire reeve (later shortened to sheriff)

The communication methods include a "bridge call" every week, where the police intelligence bureau updates security managers on current threats, recent crime trends, and upcoming events. Deployment of security officers alongside police will occur in the event of a major incident.

The modern history of executive protection begins with the formation of the United States Secret Service in 1865.

In the corporate world, executive protection is a business measure taken to preserve the organization.

Threats to an executive constitute a **business risk**

In the corporate sphere, the person who oversees executive protection may be the chief security officer (CSO) or a security manager or EP manager ranking below the CSO

The EP specialist (EPS) should develop a particular mindset that focuses on preventing and avoiding trouble rather than combating it

Six Principles of EP - Prevent and avoid danger. Realize that anyone can protect anyone. Don't stop to think. Keep clients out of trouble. Understand the security vs. convenience continuum. Rely on brains, not technology

When the trip takes place, the EPS should remember a three-part key security concept: keep a low profile, stay away from problem areas and situations, and know what to do if trouble arises

The choreography used by the EP specialist to physically move about with the subject is called "working the principal."

Security awareness means consciousness of an existing security program, its relevance, and the effect of one's behaviour on reducing security risks.

Communicate the value of the security department. A final goal of security awareness is to convey the value of the department.

OBSTACLES TO AN EFFECTIVE AWARENESS PROGRAM- Organizational culture. A security awareness program can be hindered by a culture that holds such views as "we've never done it that way before" or "we always do it this way" - Naiveté. Organizations sometimes develop a mentality that bad things will not happen to them

Policies establish rules, while procedures explain how to follow those rules

A drug is a chemical substance that alters the physical, behavioural, psychological, or emotional state of the user.

Drugs of abuse—psychoactive (mind-altering) substances—target the central nervous system and impair the user's ability to think and to process sensory stimuli, thereby distorting the user's perception of reality

Drugs of abuse include legal and illegal substances and are often consumed socially. In this analysis, alcohol is considered a drug

Drug abuse is more common among unemployed than employed persons

In 2006, among adults aged 18 or older, the rate of drug use was higher for unemployed persons (18.5 percent) than for those who were employed full-time (8.8 percent) or part-time (9.4 percent

Other than alcohol, opium may be the oldest compounded drug used by man

in the early 1800s with the discovery of two opium alkaloids: **morphine and codeine**. Morphine became popular because of its potency—one grain of morphine is about as effective as 10 grains of opium

Heroin, a morphine derivative, was first synthesized in 1898

In the 1930s it became unlawful to possess or cultivate **marijuana (Bhang)** in the United States.

The first major attempt to control opium use in the United States came in 1909 with a federal act that limited the use of opium and derivatives except for medical purposes

Later, the 1914 Harrison Act attempted to control the production, manufacture, and distribution of narcotics

methadone was used as a substitute for **heroin** in the treatment of addicts.

In 1971, U.S. President Nixon initiated a nationwide "war on drugs."

In 1988, the Reagan administration created the Office of National Drug Control Policy (ONDCP)The director of ONDCP is commonly known as the drug czar

Compared to no abusing employees, employees who engage in substance abuse may be absent 16 times more often, claim three times as many sickness benefits, and file five times as many workers' compensation claims

non-alcoholic members of an alcoholic's family use 10 times more sick leave than others, Children of alcoholics are five times more likely to become alcoholics than children of non-alcoholics

They become the 20 percent who consume 80 percent of management's time

Fronting allows users to obtain drugs even when they do not have money to buy them- For this service, employee-dealers generally charge a small premium—typically the retention of a small amount of the drug for personal use. This quantity is known as a pinch, and the practice is called pinching.

In the United States, the legal foundation for the federal strategy of reducing the consumption of illegal drugs is the Comprehensive Substance Abuse Prevention and Control Act of 1970

The Drug Enforcement Administration (DEA) is responsible for enforcement and oversees the classification of all drugs. These classifications or schedules are as follow

Schedule I. The drug or substance has a high potential for abuse and currently has no accepted use in medical treatment in the United States. Examples of Schedule I drugs are hashish, marijuana, heroin, and lysergic acid diethylamide (LSD).

Schedule II. The drug or substance has a high potential for abuse but currently has an accepted medical use in the United States with severe restrictions. Abuse may lead to severe psychological or physical dependency. Examples of Schedule II drugs are cocaine, morphine, amphetamine, and phencyclidine (PCP).

Schedule III. The drug or substance has a potential for abuse less than the drugs or substances of schedules I and II and currently has an accepted medical use in the United States. Abuse may lead to moderate or low physical dependency or high psychological dependency. Examples of Schedule III drugs are codeine, Tylenol with codeine, and Vicodin.

Schedule IV. The drug or substance has a low potential for abuse relative to Schedule III substances and currently has an accepted medical use in the United States. Abuse may lead to limited physical or psychological dependency. Examples of Schedule IV drugs are Darvin, Avocet, phenobarbital, and Valium

Schedule V. The drug or substance has a low potential for abuse relative to Schedule IV substances and currently has an accepted medical use in the United States. Abuse may lead to a lower physical or psychological dependency than caused by Schedule IV substances. Examples of Schedule V drugs are the low-strength prescription cold and pain medicines found in most homes.

Depressants include such drugs as Quaalude (methaqualone), Valium (diazepam), Librium (chlordiazepoxide), Nembutal (pentobarbital), Seconal (secobarbital), and alcohol.

In small doses, depressants produce a calm feeling and can be used for various medical purposes. In larger doses, they can cause impaired reflexes, slurred speech, and uncontrollable drowsiness. Abusers often combine depressants with other depressants or with stimulants. The abuse of depressants can lead to birth defects, overdose, and even death

Alcohol is a fast-acting central nervous system depressant that functions as an analgesic with sedative affects

In the medical sense, N**arcotics (नींद लाने वाली)** are opiates: opium, its derivatives, and synthetic substitutes. Opiates (also called opioids) are indispensable in pain relief, but they are also highly addictive and frequently abused. Opiates include such drugs as morphine, heroin, and codeine

Opiates are relatively uncommon in the workplace, as they are expensive and their physiological effects on the user are usually obvious.

In small doses, **narcotics** create effects like those of **depressants**. In larger doses, they induce sleep, unconsciousness, and vomiting.

Over the past 30 years, the prescription painkiller oxycodone has been widely abused in the workplace. It is a Schedule II narcotic

Stimulants may make employees appear more alert, eager, and productive

Stimulants Types - Among the stimulants used in the workplace are cocaine, amphetamines, methamphetamine, methcathinone, methylphenidate (Ritalin), and anorectic drugs (appetite suppressants).

Cocaine (cocaine hydrochloride) is a white, crystalline substance extracted from the coca plant

Cocaine stimulates the central nervous system, and its immediate effects include dilated pupils, elevated blood pressure, increased heart rate, and euphoria.

The high lasts only a few minutes, leaving the user eager for more. Being under the influence of cocaine is often referred to as being “wired” or “buzzed.

Cocaine’s effects appear almost immediately after a dose and disappear within a few minutes or hours. In small amounts (up to 100 mg), cocaine usually makes the user feel euphoric, energetic, talkative, and alert. It can also temporarily decrease the need for food and sleep

Cocaine-The high from snorting is relatively slow in onset and may last 15–30 minutes, while that from smoking comes quickly and may last 5–10 minutes.

Cocaine- Large doses (several hundred milligrams or more) intensify the user's high but may also lead to bizarre, erratic, or violent behaviour, along with tremors, vertigo, muscle twitches, paranoia, or a toxic reaction. Some users report restlessness, irritability, and anxiety.

Bingeing—that is, taking the drug repeatedly and in increasing doses—may lead to irritability, restlessness, and paranoia. Eventually, the user may develop paranoid psychosis, losing touch with reality and experiencing auditory hallucination

Methamphetamine is a synthetic drug easily manufactured using common materials and simple laboratory equipment. Also known as crank, meth, crystal meth, or speed, it has, in many workplaces, replaced cocaine as a drug of choice among stimulant abusers. Methamphetamine can be smoked, snorted, swallowed, or injected.

Hallucinogens are mind-altering drugs that drastically alter users' mood, sensory perception, and ability to reason. For centuries, hallucinogens found in plants and fungi have been used in shamanistic practices. More recently, even more powerful synthetic hallucinogens have been produced.

The most abused hallucinogens are LSD (lysergic acid diethylamide), also called acid; MDA (methylenedioxyamphetamine); MDMA (methylenedioxymethamphetamine), also called ecstasy; PCP (phencyclidine), often called angel dust; mescaline, which comes from the peyote cactus; and certain mushrooms.

Lysergic acid diethylamide or LSD, a colourless, doorless, and tasteless drug, is one of the most powerful hallucinogens. It was developed in a Swiss pharmaceutical laboratory in 1938.

LSD is sold as tablets, capsules, and sometimes a liquid. Ingested orally, it is called acid, blotter acid, windowpane, microdots, and mellow yellow.

Phencyclidine or PCP was originally compounded as an aesthetic for large animals. Because of its unpredictability and sometimes frightening side effects, its veterinary use was discontinued.

PCP, often called **angel dust**, comes in both a liquid and powder form. Most often a liquid, it has a strong ether-like door and is kept in small, dark bottles.

PCP sometimes causes the eyes to twitch uncontrollably, one vertically and the other horizontally. Overdose may result in convulsions, coma, and death.

MARIJUANA After alcohol, marijuana is the second most common drug of abuse in the workplace

In small quantities, marijuana produces effects like those of alcohol, and it is often substituted for alcohol by recovering alcoholics. In larger doses, marijuana can cause hallucinations, memory loss, and lethargy. When two people share a single marijuana cigarette (which takes about seven minutes), the effect is much that same as if they had each consumed six to eight mixed alcoholic beverages. The effect may last two to six hours.

Marijuana, hashish, and hash oil are all derived from the hemp plant, cannabis sativa. The principle psychoactive component, tetrahydrocannabinol, or THC, is retained in the fatty tissue of the body

Hashish consists of the THC-rich resinous material of the cannabis plant, which is collected, dried, and then compressed into a variety of forms, such as balls, cakes, or cookie-like sheets. Pieces are then broken off, placed in pipes, and smoked. The Middle East, North Africa, Pakistan, and Afghanistan are the main sources of hashish. The THC content of hashish available in the United States has increased significantly over the last decade

An analogue, also known as a designer drug, is a synthetic preparation with effects and characteristics like those of a natural substance

Prescription drugs are frequently abused in the workplace. Those most often abused are stimulants and sedatives. They may be prescribed by physicians but then overused or continued when no longer needed

The most common prescription drugs sold at work belong to the family of drugs known as benzodiazepines, which are depressants designed to relieve anxiety, tension, and muscle spasms. Librium, Xanax, and Valium are some of the more common benzodiazepines found in the workplace.

Flunitrazepam (Rohypnol) is a benzodiazepine that is not manufactured or legally marketed in the United States but is smuggled in by traffickers. Known as “trophies,” “roofies,” and “roach,” flunitrazepam gained popularity among youth as a party drug

Addiction three stages- Stage One. The first stage is characterized by an increased tolerance to the drug
Stage Two. The second stage is characterized by increases in rationalization,
Stage Three. In this final stage, use becomes an obsession.

Chemical dependency is an integral component of addiction. It is the physiological craving brought on by chemical changes in the body. These changes are both mental and physical. Substance abusers experience a craving for the drug relieved only by the consumption of it. People who are chemically dependent may lose all rationality and do anything to obtain their drug.

Another management option is to refer the abuser to an employee assistance program (EAP). EAPs first came into being in the 1940s.- Known then as occupational alcoholism programs

For which substances should the organization test? -for example, an employer may test for alcohol and five controlled substances: marijuana, cocaine, amphetamines, opiates, and PCP. These five drugs are typically referred to as the DHHS-5 (Department of Health and Human Services 5).

In federally regulated workplaces and in states that require employers to follow federal rules, **urine must be used for drug tests and saliva or breath for alcohol tests**.

The length of time drugs remain detectable in the body is called the **window of detection**

Legal drug. A legal drug is any prescribed drug or over-the-counter drug that has been legally obtained and is being used for the purpose for which it was prescribed or manufactured

Drug paraphernalia. These are items, tools, and devices commonly used in the preparation, storage, and administration of illegal drugs. Examples include but are not limited to rolling papers, roach clips, glass pipes, water pipes and bongs, drug vials, straws, and spoons, and in some cases hypodermic syringes

Serious injury. This is any work-related injury resulting in the stoppage of work and requiring medical attention of any kind

the legal system began to ask **"alienists,"** who are now called **psychiatrists**, to render opinions concerning the propensity (likelihood) of identified individuals to commit violence in the future

Like other forms of risk assessment, violence risk assessment provides information that aids in appropriate allocation of resources to minimize harm. Violence risk assessment helps differentiate between individuals who pose a threat and those who solely make threats

Like a typical security program, a violence risk assessment program employs diversion, delay, and response, but they are the last elements in the program.

For security practitioners. the most effective means of preventing workplace violence is early detection of this behavioural, emotional, and psychological dynamic.

The IMT should include, at a minimum, a senior management representative, a senior human resources manager, a senior security manager, and a legal representative who is familiar with labour and employment law and litigation

Austria and Germany have recently passed new stalking laws and are looking to use them to protect their citizens from behaviours that have not been managed legally before.

Regarding monitoring, global positioning system (GPS) technology is being used in the criminal justice system to manage offenders (via, for example, ankle bracelets). Functional magnetic resonance imaging (fMRI) is currently being explored for use in mapping brain function to detect deception in individuals.

A primary function of the security officer is access control

Observation is a prime task for the officer on patrol

Security personnel should not be required to escort visitors and customers on company property. Doing so takes officers away from their protection tasks. Whoever invited a visitor should be responsible for escorting him or her at the site

However, it is reasonable for security officers to escort people carrying large sums of money or special information or property.

Officers should also provide escorts when requested for employee safety—such as walking an employee to the parking lot at night. Officers may also escort those who need assistance due to an illness or physical disability

Three important factors relate to behaviour: courtesy, restraint, and interest. Security officers must always display the best behaviour—especially when they are uniformed in distinctive attire—because they must retain the respect of others.

A security officer may have all other personal attributes listed, but without **ethics** the package is incomplete.

The decision on whether to arm an officer should be based on the existence of one or both of the following conditions: There is a greater danger to life safety without the weapon. The officer may reasonably be expected to use fatal force.

If officers are armed, the management of the facility assumes several responsibilities- proper training of the officers to be armed selection of the appropriate firearms and ammunition proper maintenance of the firearms by a qualified gunsmith maintenance of records of the foregoing actions an adequate level of liability insurance

Storage in a reinforced building, intrusion detection, armed patrols, dual access, etc. should be considered as part of a defines-in-depth protective system. Applicable government standards and insurance carrier requirements should be exceeded in these instances.

The two reasons for testing the security operations program are to identify residual risks and identify necessary changes within the organization.

ORGANIZATIONAL STRUCTURE - VERTICAL MODEL- In the vertical model, also known as the hierarchical model, authority comes from the top or senior manager and flows down through a series of managers and supervisors until it stops with the front-line staff -The most effective managerial style for supervisors is to acknowledge credit for good performance and be objective when noting deficiencies. SHAMROCK MODEL -three-leafed shamrock-The first leaf represents a small core of professionals, managers, and skilled technicians. The second leaf consists of third-party suppliers who have been chosen for their expertise and ability to provide quality service. The third leaf consists of part-time and temporary workers who are employed as needed. Commonly known as the flexible work force. NETWORK MODEL- Also called the flattened, horizontal, or open model, the network model,

Another configuration is a hybrid security force wherein proprietary supervisors oversee contract front-line officers. In this case, the relationship is known as principal-agent.

A security officer post is any location or combination of activities for which a trained human being is necessary-That definition includes three key concepts: a location or combination of activities necessary human being training and competence to accomplish the required activities

Each post is likely to demand a combination of cognitive (knowledge), psychomotor (physical), and affective (attitudinal) skills. A human being is needed if the post requires the ability to

In addition, job-specific and site-specific criteria for physical and mental abilities should be included as screening criteria for prospective proprietary and contract security officers.

General orders may be thought of as canons or bodies of principles for protection officers.

creation of the "cry wolf" syndrome whereby a high false alarm rate causes the operator to ignore indications of system malfunction so that malfunction rates detected drop nearly to zero

Though a face-to-face interview is still the most important aspect of personnel selection, today more and more companies are investing in personality inventories, assessments, and examinations.

Code of Hammurabi, sixth king of the Amorite Dynasty of Old Babylon. The code is perhaps best known for its retributive provisions: "an eye for an eye; a tooth for a tooth.

Learning can be separated into various domains: cognitive (knowledge-based), affective (attitudinal or perceptual), and psychomotor (physical skills):

Education, then, is the foundation of training, certainly within the cognitive and affective learning domains.

First, the concept contradicts Malcolm Knowles's "principles of andragogy," a theory of adult learning that assumes adults are self-directed and will take responsibility for their own learning needs.

The case study method was developed at Harvard University in the 1880s-It has been used for the teaching of law and is also useful for guiding the learner in any topic where discretionary judgment is necessary.

In general, the **case study** method works best with students working together in groups where there is active discussion.

One method of ensuring continuous learning is to separate the training process into segments. Trainers structure their sessions with an introduction and body, then close each topic with a summary and test.

Training Obstacles- The most common obstacles are budgetary limitations, scheduling, a lack of management training expertise, prejudice, and ego

Budgetary limitations are a major enemy of training

Some managers believe they have the knowledge, skill, ability, and time to write every lesson plan and deliver every class. This belief can evolve into the **"Frog Syndrome"** (Herzig, 1993). The term refers to managers who decide to train all their subordinates personally, jump into the project, and then, when the reality of the workload hits home, jumps back out, leaving the training uncompleted. The result is that training stops, and organizational development stagnates.

Training for Intervention Procedures by Servers of Alcohol (TIPS)

Three broad criteria that a client should consider when choosing a guard contractor are the following: consistent performance prompt, efficient, and positive response to client concerns competitive pricing

A type of systems approach follows three general steps: assessment of vulnerability, implementation of countermeasures, and evaluation of effectiveness.

One definition of risk management (ISO/IEC, 2009) is "coordinated activities to direct and control an organization with regard to risk."

Although definitions of risk management vary, they generally agree that it relies on risk assessment, which in turn relies on vulnerability assessment. In addition, all definitions include threat, asset value, and vulnerability as a part of the overall risk management process. An excellent description of risk characterization, including the technical, social, behavioural, economic, and ethical aspects, can be found in Understanding Risk:

Risk assessment developed in the insurance industry, which defined risk in terms of annualized loss expectancy, which is the product of the potential loss from an event and the likelihood of the even

Risk assessment, a necessary part of risk management, is the process of defining how big the risk is. Risk assessment techniques may be heuristic (ad hoc), inductive, or deductive. In other words, some methods are more quantitative, others more qualitative

Risk assessment examines the outcome of a successful adversary attack, the likelihood it will occur, how it will unfold, and how many people will be affected. **When an entire population is at risk, it is called a societal risk.**

In risk assessment, the analyst attempts to answer three questions- What can go wrong? What is the likelihood that it would go wrong? What are the consequences?

Risk management comes next. It builds on risk assessment by answering a second set of questions: What can be done? What options are available? What are their associated trade-offs in terms of costs, benefits, and risks? What are the impacts of current management decisions (i.e., policy) on future options?

risk management is a systematic, statistically based, holistic process that employs formal risk assessment and management and addresses the sources of system failures

In general, risk can be reduced in three ways: preventing an attack by detecting it before it is under way protecting against an attack reducing (mitigating) consequences

Prevention requires intelligence gathering and deterrence. Protection requires a physical protection system.

risk control tools. Approaches include avoidance, reduction, spreading, transfer, and acceptance (Grose, 1987). A PPS is one subsystem in an overall strategy for reducing risk

Threat is a combination of adversary capabilities, equipment, motivation or intent, and likelihood of attack

After the threats and assets are defined, a vulnerability assessment is generally performed to establish a baseline of PPS effectiveness in meeting goals and objectives

Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders.

ASIS defines the design basis threat (DBT) as “the adversary against which the utility must be protected”

It is also important to differentiate security protection from safety protection. Safety is generally defined as the measures (people, procedures, or equipment) used to prevent or detect an abnormal condition that can endanger people, property, or the enterprise.

Security, on the other hand, refers to the measures used to protect people, property, or the enterprise from malevolent human threats

The key distinction between security and safety events is their cause—accidental, unintentional, or natural disaster (abnormal event) versus malevolent, intentional human caused event.

Vandals. This threat would consist of a small group of two to five unarmed people, whose intent is to deface low-value company assets or employee vehicles parked onsite

Disgruntled employee (insider). Generally, this threat would come from an individual acting alone, but there could possibly be a small group (two to five persons)

Criminals. These may be one to five people whose goal is theft of valuable property from the site; their goal is to gain financially by selling the stolen items

Extremists. This threat consists of a medium-sized to large group of people (20 and up) whose goal is to bring attention to a practice of the targeted site. Their motivation is ideological; they may be environmentalists, animal rights group

There are three general methods of valuing assets—using dollars, by using consequence criteria, or by policy

Loss impact can be measured in a variety of ways. One measure is the effect on employee morale; another is the effect on community relations. The most important measure overall is in dollars.

Costs of security losses are both direct and indirect. Direct costs include the loss of money, negotiable instruments, property, or information. Indirect costs include harm to reputation, loss of goodwill, loss of employees, and harm to employee morale.

One formula is as follows: $I = I / 365 \times P \times t$. I = income earned I = annual percent rate of return P = principal amount (in dollars) available for investment t = time (in days) during which P is available for investment

Cost-of-Loss Formula: $K = (Cp + Ct + Cr + Ci) - (I - a)$. K = criticality, total cost of loss Cp = cost of permanent replacement Ct = cost of temporary substitute CRMD = total related costs Ci = lost income cost I = available insurance or indemnity a = allocable insurance premium amount

Vulnerability assessment is the process of identifying and quantifying vulnerabilities. The term **vulnerability analysis**, which is a method of identifying the weak points of a facility, entity, venue, or person (ASIS, 2012), has also been used to describe this process. Both terms are acceptable and make the same point

The biggest mistake made when conducting a VA is to concentrate on individual PPS components and address upgrades only at that level, not at the level of the overall system

A major part of a VA is facility characterization, which is the evaluation of the facility's PPS. This is generally done with a site survey

Measures of effectiveness for entry control are throughput, false acceptance rate, and false rejection rate

A well-engineered PPS exhibits the following characteristics: protection-in-depth minimum consequence of component failure balanced protection

CPTED is the design or redesign of a venue to reduce crime opportunity and fear of crime through natural, mechanical, and procedural means.

CPTED is a set of management tools targeting the following: **Places, Behaviour. Design and use of space**

CPTED solutions as follows: **Mechanical measures**. Also referred to as target hardening, **Human and organizational measures**. These include Block Watch, Neighbourhood Watch, security officer patrols and posts, **Natural measures.** Natural CPTED measures employ good space planning to reduce inhabitant conflicts by considering compatible circulation patterns

Even when supplied by mechanical equipment (lamps), lighting is classified as a natural surveillance component.

Legitimate activity support- Some places are difficult to protect by nature of their location or other geographic features. In such instances, legitimate activity support is essential. A crime hotspot might be eradicated if police placed a substation there or maintenance staff moved to occupy the space

CPTED as it is embodied today got its start in 1973 from the early writings of Oscar Newman,

The following are several types of security zones-Unrestricted zones- Unrestricted zones might include lobbies, reception areas, snack bars, certain personnel and administrative offices, and public meeting rooms. Controlled zones. -Controlled zones might include administrative offices, staff dining rooms, security offices, office working areas, and loading docks. Restricted zones. -restricted zones may include vaults, sensitive records, chemicals and drugs, food preparation, mechanical areas, telephone equipment, electrical equipment, control rooms, laboratories, laundry, sterile supply, special equipment, and sensitive work areas.

The first step toward CPTED-based parking lot security is the vulnerability assessment

recommends lighting levels of 5 to 6 foot-candles (54 to 65 lumens per square meter) in gathering areas such as stairs, elevators, and ramps. Walkways around garages should have 5 foot-candles of lighting.

Open parking lots should have a minimum of 3 foot-candles (32 lumens per square meter)

Most CPTED practitioners prefer metal halide lamps because they last about 20,000 hours and accurately reproduce the colour of cars, clothes, and people.

Low-pressure sodium vapor lamps typically last about 50,000 hours and are the most energy-efficient, but their poor colour rendition makes them unsatisfactory for capturing crime scene details

High-pressure sodium vapor lamps and mercury vapor lamps are less expensive than metal halide lamps but do not last as long and do not render colours as well.

For example, wall surfaces can be coated with graffiti-resistant epoxy paint, and lighting levels can be increased in problem areas to increase the potential for natural surveillance. Attempts to prevent graffiti tell vandals that the property is the territory of its rightful owners.

CPTED is a legitimate strategy for reducing the opportunity for acts of terrorism as well as more common criminal acts.

Sensors are the basic building blocks of an intrusion detection system.

All logical discrimination, transmission, processing display, and recording activities that occur after the initial alarm are due to the technology on which the sensor is based, including optical, electronic, electromechanical, or mechanical capabilities.

Intrusion detection is the process of detecting a person or vehicle attempting to gain unauthorized entry into an area.

Three main characteristics of intrusion sensor performance are probability of detection (PD), nuisance alarm rate, and vulnerability to defeat

A perfect probability of detection would be 1. However, in real life a sensor's PD is always less than 1. After thousands of tests, a sensor's PD only approaches

For any specific sensor and scenario, the two values PD and confidence level (CL) are used to describe the effectiveness of the sensor

The perimeter intrusion detection system shall be capable of detecting a person, weighing 35 kilograms or more, crossing the detection zone by walking, crawling, jumping, running, or rolling, at speeds between 0.15 and 5 meters per second, or climbing the fence at any point in the detection zone, with a detection probability of 90 percent at 95 percent confidence.

Occurrence of a potential intrusion event. These are intrusion sensors. A change in a safety or process condition being monitored (rise in temperature, presence of smoke, etc.). These are state sensors. Loss of electrical power. These are fault event sensors. Opening, shorting, or grounding of the device circuitry or tampering with the sensor's enclosure or distributed control panels (transponders). These are tamper sensors. Failure of the sensor itself. This is another fault event that should be detected.

exterior intrusion sensors-five methods of classification are used- passive or active covert or visible line-of-sight or terrain following volumetric or line detection application

Types of active sensors include microwave, infrared, and other radio frequency (RF) devices.

They transmit energy and detect changes (caused by the presence or motion of a target) in the received energy. Active sensors typically contain both a transmitter and a receiver

The use of exterior perimeter sensors is generally limited to government, nuclear, or correctional installations.