CEP C 1 2023.2-Doc 6.Annexe 4
(CEP C 1 GSP 2023.2-Doc 5c.Annexe 1)
مجلس الاستثمار البريدي- اللجنة 1- 2023-2-
المستند 6- الملحق 4
(مجلس الاستثمار البريدي- اللجنة 1- فريق الأمن
البريدي- 2023-2- المستند 5ج- الملحق 1)

يرد باللغة الإنكليزية

Guidelines for Postal Crime Prevention

UPU Postal Security Group

Version 1.1

Berne 2023

UPU International Bureau

Stl/Hd

Table of contents Page

1 Introduction

Electronic communication and new technologies have dramatically transformed the way postal services conduct their business. After historically operating as protected monopolies, postal services are now competing in a more challenging environment where customers and marketplace pressures determine whether postal operators succeed or fail in their business objectives.

If postal operators wish to remain viable business entities, they need to do everything possible to ensure that core and premium products and services provide features that represent equal or better value than those of their competitors. A basic requirement in this environment is that services, products and finances be available, safe and protected, and that those working in the postal environment, as well as customers, feel secure and valued.

Postal operators internationally have a unique opportunity to support the growth of the postal business through quality security initiatives, which will further enhance the quality of the services provided to customers.

Considering the globalization of commerce and e-commerce, it is now more necessary than ever to provide a quality, secure postal service, not only within the sphere of an individual operator, but within the international network as well. Critically, in this context, it is essential to develop and establish a greater understanding of the principles for preventing acts of criminality and dishonesty throughout the postal environment.

While it is a common practice to conduct criminal investigations in a reactive fashion, where the focus is largely upon determining the identity and methods of an offender, it is equally important to recognize the necessity of effective proactive prevention strategies to encourage customer and employee confidence in the Post. These strategies should be undertaken with a holistic approach where crime prevention, investigations and criminal intelligence individually fulfil a critical role within the development and establishment of effective crime prevention.

The purpose of this document is to provide a focused, step-by-step approach to ideas and strategies for crime prevention for all Posts, serving as a kind of a checklist for security issues. At the same time, it will attempt to provide general guidelines of value to the diverse membership of the UPU, containing solid information and proposals. Lastly, the issue of the bottom-line value and necessity of effective prevention strategies will be addressed, recognizing that if products and services are not protected, they cannot be available to postal customers.

The intended audience for this document is, of course, security and law enforcement professionals within the UPU membership. It is also designed to provide ideas and insights for postal managers, employees and external colleagues who assist in protecting Posts, customers and employees. The strength and survivability of the world's Posts depends first and foremost on security and prevention to protect their valued assets.

2 Overview and objectives

For crime prevention to work in an organization or business, it is essential that a holistic approach be achieved whereby all elements are interlinked with each other. The following are some of the major aspects that need to be addressed in a successful crime prevention strategy:

– Successful reactive investigations serve a dual purpose in crime prevention by bringing offenders to justice and by determining the possible security weaknesses that contributed to the crime;

– A successful crime prevention strategy will educate and involve all employees at all levels as to their role and responsibility with regard to safety and security and the advantages to them of a more secure work environment;

– An inclusive approach of employee education and awareness will develop a sense acceptance and commitment among employees that makes them the first line of security and prevention;

– Physical security does fulfil an important role in enhancing the safety and security of company employees, assets, equipment, customers, etc.; however, effective management at the operational level will ultimately determine the success of implementation;

– An effective crime prevention strategy balances minimum necessary control with maximum employee acceptance and support;

– Understanding the reasons for crime, while a very complex matter, can bring focus to developing a crime prevention strategy;
– Objectivity, accountability and professionalism of security and investigation service personnel have a positive impact upon the development of employee support, acceptance and assistance;
– Communication throughout the organization (both up and down the hierarchy) as well as with customers, associates and related organizations as to security needs and how to achieve them is essential to an effective strategy;
– Crime cannot be effectively detected and prevented within an isolated environment. As such, partnership development (internally and externally) as well as community involvement is of critical importance;
– A “team approach” through a clearly understood and accepted prevention strategy with specific responsibility and proactive, quality- and project-driven targets will have the best chance of success. A positive problem-solving attitude should be established;
– It is the security professionals’ responsibility to communicate effectively with employees and management as to the risks and benefits involved in security and prevention.

A sound crime prevention strategy is not merely an approach based on physical security measures; it is a broad concept where the basic requirement is to develop and implement constructive strategies, countermeasures and action plans. Obviously, no security plan will be infallible, and there will always be criminal attacks to be dealt with, but an effective approach will allow security specialists to learn from new challenges and procedures for continual evaluation, and review must be built into the prevention plan.

Crime prevention is broadly based on the following principles:

– An assessment of the value and vulnerability of entities requiring protection;
– An assessment of the threats, risks, opportunities and influences in the environment that could lead or have led to criminal activity;
– The development and implementation of countermeasures, strategies, systems and/or procedures which would reduce the desire and opportunity for criminal activity;
– The ongoing evaluation of the existence and effectiveness of the countermeasures, strategies, systems and/or procedures that have been implemented;
– Educating customers, employees and others involved with the Posts to report incidents to the appropriate authority for record keeping to further assess the situation and take proper measures to resolve the issue;
– Generating and maintaining awareness and responsibility among all employees.

The most fundamental objective of crime prevention is to establish general awareness and accountability among all levels of management and with all employees within the company. This is a concept that is easy to understand but difficult to achieve and maintain, and is the primary challenge for security professionals.

3 Risk assessment

Assets within a business or corporation include money, stocks and inventories, property and buildings, equipment and, most importantly, employees. In addition, there are non-physical assets, such as customer confidence, brand recognition, corporate/proprietary information and data, and community standing. All of these assets can be diminished or lost through the many threats of criminal activity that an operator faces. In the case of employees and customers, they represent both the essential elements of business operations and potential sources of risk and threat. As such, they must be supported and protected while at the same time being restricted from having the opportunity to engage in unlawful or dangerous activity: a sometimes difficult but necessary balancing act for security professionals.

The initial concept of security awareness and prevention is risk assessment. This should, of course, always be directly connected to the value and exposure of assets. Since risk comes in multiple forms and changes constantly, there are various techniques and principles to be considered in evaluating risk. While it is certain that all risk cannot be eliminated, the challenge for security specialists is to remain ever vigilant to the organization’s exposure to risk and to constantly re-evaluate and modify their security strategy as situations change, which they always will.

A substantial part of this document will focus on this essential area of risk assessment as applied in a focused way to the protection of the various assets and services that make up a modern postal operator. In addition, suggested approaches will be offered to reduce exposure and risk, while recognizing that it is impossible to identify and eliminate all risks, just as it is impossible to cover all potential approaches to controlling or eliminating risk. As always, the most important tool of the security specialist is their professional judgement, informed by experience and analysis.

The following areas of asset exposure and risk assessment will be covered in detail in the sections below:

– Buildings and facilities, with a focus on preventing unauthorized entry and external attack;
– Equipment and prevention of theft and sabotage;
– Mail theft and threats in the mail;
– Financial assets and internal/external theft and embezzlement;
– Employees and threats to and from them;
– Customer protection and access control;
– Other occupants of shared facilities and access control;
– Misuse of Posts, including harmful items, stamp/meter counterfeiting, fraud, mail bombs, pornography, drugs and other prohibited items;
– Law enforcement assistance and cooperation;
– Security services contracting.

4 Techniques and principles of risk assessment

A proper starting point for the assessment of risk is to attempt to establish a valuation of property and assets and the costs of replacing or doing without those resources. In one sense, security can be regarded as concentric circles, with the highest level of protection to be afforded to irreplaceable resources and to property and assets that are most costly, indispensable and time consuming to replace. The basic question of what needs to be protected and what level of protection to provide must begin with a survey and analysis of existing buildings/facilities, personnel, equipment, mail, finances and inventory. A survey and analysis of this information should require input from management. It can have the secondary benefit of helping them understand the risk to essential assets for which they are also responsible, and the potential harm to the organization if such assets are lost or compromised in some way.

It should be clear that, just as security staff are not solely responsible for security, they also could not be the sole source of pertinent data, information or analysis with regard to security threats and risks. A network of input from management, employees, law enforcement, and the community must be relied upon in order to conduct successful risk assessment. It is important to carry out the necessary research and develop valuable contacts in order to provide the elements of effective analysis.

An invaluable source of information for effective crime analysis and risk assessment is law enforcement. Local law enforcement can be relied upon to provide information and insight concerning threats and criminal activity in the community where a facility operates or is planned. Where national or local law enforcement crime statistics are available, they can be an essential tool for evaluating risks in various areas and communities. Law enforcement contacts should be developed and nurtured as an important resource for crime analysis as well as a valued partner in responding to threats and attacks.

In addition to law enforcement tools for conducting community analysis, it is important to consider other sources of information with regard to risk assessment. For example, community and neighbourhood organizations may be able to provide unique insights and information. Available data such as sociological studies and analyses as well as environmental studies of population density and makeup, available services – such as police and fire protection – and other pertinent reports and information can be considered. Obviously, the makeup of a community and its relative urban/suburban/rural mix has a significant potential influence on the degree of threat and risk and, in turn, on the related security approach.

An essential specific tool for security professionals is the security survey. Any effective risk assessment must be conducted through the use of a well-designed survey to help guide the inquiry in a logical way. If a survey format has not been developed (or if a draft survey form exists) it would be in the best interests of those who will be responsible for carrying out the risk analysis to begin by setting out their plan of action. This should take the form of a survey designed to address the specific objectives of their review. In developing an effective survey format, it is good practice to receive input from as many varied viewpoints as practicable.

This should ideally include input from management and employees, as well as diverse expertise from the survey team. Consideration can be given to utilizing questionnaires to develop diverse information from management, employees, customers and the community to the extent desired. The important thing to keep in mind is that pre-survey input and analysis can aid security specialists in developing a realistic and focused survey format that can serve as an invaluable roadmap and checklist to ensure a successful and valuable review. This approach also has the benefit of increasing involvement and acceptance from all those who are consulted and participate. While specific security survey formats will vary widely depending upon the nature and purpose of the review, the essential point is to have a logical plan that addresses key concerns, risks and opportunities identified by the survey's clients/customers and the review team.

5 Buildings and facilities

When most people think about security, they think in terms of physical security of buildings, plants and facilities. This is a reasonable place to begin thinking about the application of security guidelines. However, as we will make clear in the remainder of this document, it is only a starting point. and the issues of building and facility security, as well as the issues involved in a comprehensive overall security approach, are complex. Moreover, when people consider the security of buildings and facilities, they all too often think in terms of after the fact, or following construction security reviews. Instead, security guidelines and standards can be applied to new facilities at the outset, which will be less costly for appropriate modifications. As security specialists, it is important to remember that there is no such thing as perfection and that the increasingly competitive postal environment requires the use of rigorous cost–benefit analysis even in the crucial area of security. In emphasizing security to senior management, moderation is key, and it is often wise to have various levels of protection identified with a solid analysis of the costs, benefits and risks of alternative approaches.

Security awareness should be applied to buildings and facilities at the earliest stage of planning (i.e. before construction). If feasible, risk assessment should be addressed at the site location and evaluated before construction begins. As mentioned earlier, good security awareness depends on effective communication and cooperation throughout the postal business. Therefore, a good partnership should be developed between the responsible security officials and the managers responsible for site selection, real estate acquisition, architectural development, and plant construction. While the objectives and responsibilities of the different managers involved in these areas do not always coincide, cooperation and support are beneficial to the overall interest of the business.

In evaluating prospective building sites, it is important to use the appropriate techniques and principles of risk assessment discussed in section 4 (above) to answer key questions.

– What is currently at the site location?
– What is the population density and make-up?
– What is the criminal activity in the area?
– What other facilities are in the area, what problems have they experienced, and what is their level of security?
– What is the physical environment like, and what are the advantages and disadvantages that need to be addressed in facility design and construction?
– What other threats could occur (e.g. power failure, fire, building collapse, water damage)?

As part of the architectural review, it is good to consider what reasonable modifications to overall design might best enhance security and provide safety for employees, infrastructure and customers. This review should also include consideration of the placement of cameras and other surveillance devices, access controls, entry and exit flows, fencing, signs, landscaping, parking, and other possible security modifications or enhancements. Interior layout of the facility is also important from a security standpoint, to identify what will be protected, determine the value of the building, its contents and services, and establish how access will be controlled within the interior of the plant.

A basic principle for security managers is that security begins on the perimeter of a facility and works inward through layers of access towards the most sensitive areas where the most valuable assets are protected. The first line of protection is the perimeter. As we consider perimeter security, the fundamental question is who will have access and how that access can be controlled. Facilities open to the general public will have different perimeter controls from specialized plants holding high-value assets and property. It is the responsibility of security officials, working with management, to identify the proper level of access and perimeter control. In looking at fencing, for example, all options should be considered, including signs, decorative fencing (to mark off areas and subtly limit access) and barbed wire (including an alarm or electrical fencing), along with the option to combine physical security features with guards (armed or unarmed). It all depends on what is being protected, who needs access, and the nature of the surrounding area. In looking at fencing and perimeter control, it is also helpful to consider the immediate landscape of the area, including trees, vegetation and terrain.

The next level of security following perimeter control and fencing is access control. Based on the value of assets and required accessibility, consideration should be given to the proper level of access control. For example, are turnstiles, gates, metal detectors, photo-identification cards, electronic ID badges that can track movement, or other devices appropriate to the desired level of control used? In addition to entry access, it is also important to manage exit control in some situations to limit opportunities for theft or unauthorized entry, while recognizing the need for clear emergency exits with alarmed doors. Other effective tools for access control are simple ones, like signs that direct or restrict access, to more complex systems, such as camera and alarm systems and recognition technology. Security guards are also often an invaluable resource for effective access control. It should be kept in mind, however, that the higher the level of security, the higher the cost. Whichever access system is adopted, it is important to include efficient and considerate procedures for receiving disabled people, customers, visitors, other building or plant occupants, and walk-in traffic.

A special area of consideration with regard to perimeter security and access/exit control is how to handle vehicle traffic and parking. Vehicles present a potential threat because they can be used to carry unauthorized items and people into facilities as well as to haul out stolen goods, equipment, mail or property. In addition, vehicles (with or without the knowledge of the driver and occupants) are one of the more widely used and effective devices for carrying terrorist bombs into or near facilities. For some, the connection between postal installations and the government can make facilities an attractive symbolic target, especially if security weaknesses are obvious. One method that could be considered is to screen (and perhaps search) vehicles that enter and leave postal facilities, again depending on the risk and sensitivity of the facility. This should be balanced with privacy concerns and efficiency.

Throughout the discussion of the appropriate level of perimeter control, it is important to bear in mind that the degree of control should be based on the level of risk and threat as identified through rational use of techniques and the principles of risk assessment. Even though there is no easy solution or guarantee that a system designed to identify realistic threats of unauthorized penetration, sabotage and terrorism will be effective, risk assessment should still be pursued.

Beyond the concern with exterior perimeter protection, it is also important to remember that within the facility, as mentioned earlier, there are other layers of security with varying levels of appropriate access control that can vary from area to area and room to room. This can sometimes call for different levels of access badges to maintain proper security protocols. Moreover, the need for special “strong rooms” to control cash and high-value items and mail should be considered. Generally, these types of rooms should be in the interior of a facility to reduce the opportunity for robbery and should be equipped with access controls, cameras and systems to maintain strict accountability.

Another important area that can be overlooked in assessing building and facility security is the control of keys. Lack of key control can diminish the overall security of a plant, and it is essential that procedures be developed for assigning, inventorizing and transferring keys, as well as controlling their duplication. Proper accountability also calls for strict procedures for handling lost keys. The use of a dual key system in especially sensitive locations, where two accountable staff members must coordinate to have access to high-value items, should be considered, as appropriate. Moreover, combinations for locks to vaults and safes must be controlled and changed periodically, and especially when employees are transferred or leave.

Buildings and facilities that are not occupied on a 24-hour, seven-day-per-week basis should be considered as potential targets for burglary. Burglary prevention should be built into facilities to the extent possible. For example, good lighting and clear perimeter sight lines represent a strong deterrent to burglars. Attention should be given to shrubbery and landscaping surrounding buildings. An alarm system is also an effective tool and deterrent, especially if there is a rapid response capability by law enforcement or security officials. The installation of cameras can aid in discouraging and identifying burglars. Community burglary prevention programmes, such as neighbourhood watch, where communities work together to discourage crime, can also be considered a potential resource for burglary and crime prevention.

Lastly, as part of a good security approach it is wise to develop and update, with responsible management, contingency plans to address threats such as natural disasters, fires/explosions, evacuation procedures, responses to bomb threats and violent incidents, etc. Thinking and planning ahead can reduce panic and confusion if something does happen, thus enhancing overall employee and customer safety and confidence.

6 Equipment and technology

Modern organizations have a greater dependence on costly equipment and technology. The interconnections among equipment, technology and people are crucial for achieving efficient production, measurement and control. However, this growing risk of equipment theft or sabotage poses a significant threat to modern enterprises. Over the past few decades, competitive pressures and the need to be more efficient have led to increased reliance on technology within the world’s Posts. This has resulted in an increase in risks in the following three principle areas:

i Equipment or technology is sometimes seen as a threat, owing to factors like redundancy, where some disgruntled employees may feel justified in sabotaging plant equipment as a way of striking back.

ii The growing cost and value of equipment has increased the risk of theft.

iii Complex technology can sometimes be used by bad actors to falsify data, in areas like productivity, or to conceal theft or embezzlement.

As in all areas of security prevention, the described risks are not just within the purview of security specialists, but are also the responsibility of overall management, and should be addressed in partnership with colleagues. It is recommended to take a coordinated approach to ensure the safety of employees by proper placement, utilization and maintenance of equipment. Likewise, with the use of technology to control and account for assets and productivity, it is important to work with managers to develop and maintain systems (e.g. accounting and auditing) and introduce methods of protection against vulnerabilities leading to potential acts of sabotage and hacking.

The placement of equipment is an important consideration in pre-construction and renovation surveys. Equipment that is expensive and contains essential technology should be positioned in areas where it can be protected and subject to the required surveillance. Consideration should be given to granting limited access to equipment to only those with a need and authorization. Tools such as access control, alarms, cameras, passwords, and card-reader technology are examples of other security measures that can be employed. Another important consideration is maintaining a good inventory system and identifying equipment with serial numbers. Where employees, contractors or customers are authorized to remove equipment from facilities, a system should be in place for tracking and control. Lastly, proper maintenance schedules and records should be kept to ensure the safety of the equipment, as well as the ability to establish proper accountability.

7 Mail

For the world's Posts, the most essential services ensure the safe, swift and reliable handling and transportation of mails. Given the value and potential exposure of vast volumes of mail moving all over the world, there are innumerable threats of theft, robbery and destruction. Risks come from different angles, such as internal as well as external threats, and are impacted based on the volume of mail, its value, and the complexity of mail flows (e.g. routes and networks). This creates a major challenge for security professionals and can be discouraging, with the realization that losses will likely occur in such a vast operation. However, such realizations should not diminish efforts in meeting that challenge.

Among the complexities of the mails is the fact that their intrinsic value varies greatly. While all mail is important, there is a difference between high- and low-value mail that is recognized by potential thieves. There is a basic need to develop and maintain a system of separating and providing defences for high-value mail and shipments. Most Posts have different mail classifications for registered, insured, certified, and other special mail

services. From a security standpoint, it is important that these classes of mail receive the appropriate level of protection. Procedures for registration, numbering, receipting, hand-to-hand accountability, and tracking should be verified and audited on a regular basis. The movement, storage and transportation of such items warrants appropriate attention, with consideration given to the need for escorts and guards. Within facilities, proper security in handling areas (such as security cages) should be set up and regularly evaluated, as should the need for enhanced access controls, cameras, alarms, etc.

During transportation, mail is especially exposed to theft, damage and destruction. Special consideration as to the effective use of security containers such as mailbags, locks and seals has often been a focus of the UPU Postal Security Group (PSG). In addition, systems of tracking high-value mail and the use of hand-to-hand accountability are important security prevention techniques to be considered.

Parcels often present an especially attractive target to thieves because of their potential value. Special handling and storage procedures may be warranted. In addition, parcels present a different threat from regular mail in that they are more likely to contain prohibited and dangerous goods and bombs. More attention will be given to this consideration in a later section.

Mail leaving facilities to be delivered by carriers is at even greater risk and presents a special threat to employees. Robbery of carriers and theft from collection and mail-relay boxes are major problems in some areas. Delivery employees should be well trained in how to remain alert to prevent a robbery and how to respond for their security and protection, while recognizing how to be an effective witness in a potential investigation. Employee safety is the primary consideration. Separate procedures may be warranted for handling cheques, cash, and other high-value items depending on the assessed risk in certain areas. On days when a number of cheques are delivered, extra security or law enforcement presence may be considered if available. Collection and mail-relay boxes should be secured and reinforced to the extent necessary to prevent theft, and keys should secured appropriately.

Mail that is temporarily out of the hands of postal services and under the control of contractors and airlines for transportation often presents particular difficulties for postal security officials. It is essential to work with postal contract administrators and managers, as well as contractors and airline officials, to ensure a proper level of security, accountability and control. While this can be a delicate area, it is important to focus on such issues since the contractors or airlines often have control over contractor hiring and background checks, the viability of transportation, storage, and security systems. If possible, it is beneficial to perform periodic security surveys, preferably with the support and participation of personnel from the contractor and airline/airport security, to evaluate and enhance protection for mails entrusted to their care. As in all areas of security, partnership and a team approach is the goal.

8 Finances

Cash and financial instruments present the highest risk for the reason that they are most attractive to thieves and criminals. Given this attraction, and the fact that the loss or theft of such assets can greatly impact the fiscal health of an enterprise, it is very important that an effective system of revenue protection be implemented and maintained. The most obvious risks to cash assets are theft, both internal and external, and robbery. Posts that also provide financial or savings services for customers are often at the greatest risk. While internal theft by postal employees can usually be addressed by good internal controls through cash management and a system of audits, external theft and robbery presents its own challenges, with the added risk of potential harm to employees and customers.

As with other components of developing security measures, robbery prevention techniques begin with good risk assessment and analysis. It is important to know the neighbourhood and level of criminal activity, the value and flow of cash assets being protected, and the vulnerability and attractiveness to criminals of facilities and window services. After surveying these areas using good techniques and principles of risk assessment, security officers and management can address vulnerabilities. Training employees who are at risk in high-target areas is essential. Their safety in the event of a robbery is the priority. Training will also put in place procedures to protect assets and aid in possible investigations (an important deterrent to future crime).

Physical modifications such as counter-activated alarms, use of “bait” money or money orders, surveillance cameras, and bulletproof screen-lines (especially in high-risk facilities) provide additional protection and can enhance investigations. Well-trained lobby security guards also serve as an effective deterrent to potential perpetrators. As mentioned earlier, consideration should also be given to handling high-value items in the mail and storing cash in strengthened rooms well inside the facility to limit access. Moreover, management should be aware that good financial management and revenue protection means limiting the amount of cash on hand to the extent possible in window operations to reduce threat and loss.

Good financial management and revenue protection are also necessary for reducing the risk of employee embezzlement, theft and loss. To lessen the chance of criminal activity by employees, clear procedures of accountability and control must be in place, and employees need to be well trained in their financial responsibilities. This should be backed up by a system of audits, both routine and surprise. The use of surveillance technology, such as cameras, and access controls can also serve as a deterrent to theft.

The accumulation, storage and transportation of cash assets are especially important considerations. As far as possible, cash accumulation should be limited. Secure storage vaults and safe equipment (with good control procedures) are essential. With the transportation of large volumes of cash, consideration must be given to the method of shipment, including the type of vehicle used, and whether to use outside courier services, escorting, etc.

While stamp stock is not as readily attractive to thieves, it is still a targeted asset with clear risks for postal services. Loss of stamp stock, through theft or embezzlement, has a negative influence on a postal corporation’s bottom line, as does loss through financial theft. The same kinds of accountability systems, storage and transportation procedures that apply to cash should be provided for volumes of stamp stock. It should also be kept in mind that manipulation of stamp stock is sometimes used by employees to attempt to mask other financial embezzlements; this should be addressed as a possibility in internal audit procedures. Lastly, attention should be given to the risks involved in the printing and destruction of postage stamps. Facilities that produce stamps should be subject to rigorous controls with on-site surveys and periodic reviews to ensure their accountability and the effectiveness of their procedures against theft or conversion. An effective system for destroying old stamp stock should also include periodic reviews with clear procedures and controls for preventing theft or conversion by responsible employees or contractors.

9 Employees

An effective security prevention programme depends on the understanding and support of employees at all levels of the organization. While everyone wants to work in a safe and secure environment, the difficulty is in developing the specifics of a security programme that gives employees a sense of involvement and responsibility along with supportive management values. Involving everyone in the programme through consultation, education and awareness may be challenging but it is also essential. Teamwork is key.

The challenge with regard to management commitment is to convince leaders that security makes good business sense; that a strong bottom line depends upon loss prevention and safety for employees and customers. The first step in meeting this challenge is for security specialists to do their homework and, through good risk assessment techniques, identify the specific threats that exist in the work environment. Security officers should meet with senior managers to educate them on existing and potential risks and provide practical suggestions with cost estimates for addressing those risks. The ideas, views and desires of management must also be solicited in order to gain their support and commitment.

Once commitment from senior management is obtained, the same process of consultation, education and sharing of ideas should be carried forward with middle managers and first-line supervisors. These managers can present a special challenge because they are often stretched thin with regard to resources, and already view themselves as having abundant responsibilities and being pulled in multiple directions. An approach of understanding, listening, and being open to reasonable “real-world” compromises can go a long way to reducing resistance and gaining middle management and supervisory support. This is also an area where having the support of senior management is essential.

Employee understanding, involvement and commitment are also essential elements of a well-functioning security prevention programme. In many ways, employees are the first line of defence. This is why it is important for employees to have good security awareness and have processes in place to document and report incidents. Workers should be encouraged to watch, listen, respond to, challenge and report security breaches at the earliest stage of detection. With these measures in place, prevention efforts will be more effective and efficient. The key to achieving this is having a strong security awareness programme backed up by continual support and reinforcement through multiple approaches and techniques, such as the following:

– Providing security orientation for new managers and employees, with periodic follow-up briefings and training to reinforce security awareness and responsibility;

– Developing security improvement suggestion programmes, with well-publicized contact numbers, appropriate rewards and recognition, and reported feedback on successes;

– Producing written material, including instructional or advisory material, reminder posters, agreements, acknowledgements and, of course, written security policies and procedures;

– Using audio-visual material, such as media clips, flyers, posters, PowerPoint presentations, or a combination of informational material at meetings, where employees congregate (cafeterias, break areas, etc.), or at informal or stand-up meetings to address awareness themes;

– Integrating security into line management operations and goals (with the agreement of senior management), by including specific coverage of security performance in merit and promotional reviews, bonus or incentive compensation awards, and during routine or special supervisory and management staff meetings;

– Including security in job descriptions and recruitment notices;

– Conducting security reviews and sharing results, both positive and negative;

– Sharing available information about identified threats, crime statistics, and trends concerning specific offices or areas;

– Conducting crime prevention forums and events for all levels of the organization, in order to encourage understanding, responsibility and participation within offices;

– Releasing crime prevention notices;

– Benchmarking security standards and adopting best practices throughout the office or organization;

– Maintaining a positive security presence and availability in work areas to encourage contact with employees and let them know security is there for their benefit.

To enhance the probability of success of the above initiatives, it is important to work with and gain the support of other groups within the enterprise, such as the training section, employee and labour relations personnel, and communications staff.

Working with organized labour unions and employee organizations can present a sensitive challenge for security managers, but it is important to focus on the fundamental principle that security is good for everyone in the organization. With organizations remaining vigilant about crime and safety in the work environment, it can increase opportunities for a collective and coordinated approach to crime prevention. The support of organizations and their ability to communicate effectively with the employees they represent is a key to the success of security programmes. However, it should be clear that final decisions about security rest with the designated security professionals and their senior managers.

An important consideration for employee groups, managers and workers is safety, and a direct association can be drawn between safety and security/crime prevention. As part of a security programme, emphasis can be placed on the goal of safety as a driving force. Managers should understand that security personnel can be their eyes and ears when it comes to safety violations and unsafe procedures or hazardous conditions, such as blocked exit doors, exposed machinery, hazmat, etc., and these areas should be covered during reviews. Not only does the presence of security officers provide a sense of safety to employees, but security officers who are friendly and attentive can be seen in a positive light by employees.

As has been emphasized throughout this document, fellow employees are essential allies and partners in security prevention programmes, and many of them are supportive of a safe, secure and crime-free work environment. At the same time, a small number of people in the workforce present a potential threat to the welfare of all and the viability of the enterprise by engaging in criminal or dangerous activity. These activities can include theft, violence, sabotage, or even participation in external criminal attacks by serving as informers for “inside jobs” or as co-conspirators.

Given the potential for harm from a few employees, it is an unfortunate necessity that security controls of varying degrees – based on risk and threat – must be put in place. While the idea of control sometimes has negative connotations, it is important to deal with these perceptions among managers and employees in a direct manner, while at the same time taking a fair and measured approach. Meeting with employees and their representatives when security changes are being considered can have a positive effect to gain understanding, support and cooperation. Good control procedures can be viewed as necessary and positive, as well as being beneficial to employee safety and organizational sustainability.

Good security control procedures begin during the employment process. Pre-employment background checks that are periodically updated can screen out undesirable individuals from the workforce. Once employees are hired, it is important to begin with a thorough orientation process and effective job training that covers the need for and importance of safety and security procedures. Crime prevention training and briefings that address areas such as robbery, theft, awareness and prevention, as well as the importance of good fiscal controls, can prevent problems from occurring. The continual involvement of employees, with refresher training and briefings, along with accessibility to open and attentive security personnel, can pay dividends in employee support for prevention and security.

With good communication and employee engagement, employees can be educated about the importance and benefits of control procedures, such as identification badges, access controls, metal detectors, restrictions to certain areas, and separating dining and break areas from work facilities. Employees can also be encouraged to report criminal activity and unsafe conditions, to challenge unauthorized visitors and intruders, and to advise appropriate authorities of suspicious situations. Vehicle access control and security in parking areas is also necessary.

In addition to proper hiring controls for permanent employees, appropriate attention should also be given to contract employees and their access to facilities. As part of contract negotiations, contractor hiring procedures and background review policies should be explored, particularly for more sensitive contracts. Access control for contractors and other workplace visitors should be no less rigorous than for regular employees.

When security reviews are conducted at facilities, employees and managers at all levels should be included in the process and advised of the results, both positive and negative. This can be done through interviews, group meetings, questionnaires, written reports, presentations or videoconferences. This may seem logistically burdensome, but the benefits in quality of input into the review and acceptance of results will be significant. As an option, the review process can include contact information for employees, or they can also remain anonymous.

It is sometimes necessary for security professionals to be involved with employee interactions such as disciplinary procedures, employee removals, and criminal prosecutions. While not a common aspect of the job, it is essential that problem employees be dealt with promptly, fairly and efficiently. This requires careful and comprehensive notes, surveillance, interview records, and proper care of evidence. It also requires good relationships with management and other law enforcement representatives, while maintaining a level of professionalism in dealing with the problem employee. While the impact of a removal or prosecution can be a positive boost to security awareness and even increase employee support for crime prevention, the issue must be handled with delicacy and full adherence to legal principles and fairness.

10 Customers

Along with employees, there is the need to protect customers from physical harm while in postal facilities. Unsafe situations can result in serious loss of customer confidence and legal liability, and can cause serious harm to the Post’s reputation and image. Moreover, Posts must also protect customers from harm, as bad actors sometimes utilize postal products and services to facilitate their schemes, such as mail fraud, mail bombs, and other unsafe, harmful, illegal or objectionable contents. Customers must be protected from criminality by those few postal employees who violate their trust by stealing or destroying mail entrusted to the postal system.

Good communication and customer outreach in the area of security can help Posts serve and protect their valued customers while at the same time limiting postal exposure and risk. It is important that customer access be limited to business areas using access controls and good directional and information signs, along with employee availability to assist them as needed. Good customer communication also includes customer education and outreach programmes. Written brochures and posters, for example, can give customers good advice and guidance, from the services available to the ways in which they can protect themselves. Working with public information/affairs personnel and customer service staff can be helpful in this regard. Open public forums where customers are invited to share information, observations and opinions can also be beneficial. Customer surveys can be useful in addressing security issues, needs, ideas and expectations.

While the goal is for all customer contact to be positive, this is not always possible, and developing a system for customers to communicate their concerns, complaints, suspicions and problems is essential. A customer complaint system can also address security prevention issues and potential criminal or unethical activity. Availability of a customer complaint/information system should be well advertised and easy to use. Contact individuals and numbers should be clear and easily accessible with provisions for anonymity, if desired. A reward/recognition programme can be valuable (for customers as well as employees) if well administered.

Addressing security and crime concerns with customers in an open and positive manner is good business. It expresses a sincere concern for customer welfare and safety and places them on the same side – as potential eyes and ears for helping the Post remain aware of threats, breakdowns in security or procedures, and for reporting suspicions of criminal and unethical activity. This kind of customer/corporate partnership strengthens bonds of trust and mutual support. At the same time, Posts can educate them as to their security needs and explain any restrictions those needs impose. Management at all levels can appreciate and support this kind of positive customer service approach and see the benefits that crime prevention and security can bring to the postal business.

11 Other occupants, neighbours and community

In instances where other businesses or organizations share space with postal operations, it is important to consider how best to work with those entities to make sure that their employees are not at risk and that whatever potential threat they might present is limited. This can be a delicate matter because authority over the employees of an occupant business is limited. The best place to start is by meeting with managers from the other group to explore mutual needs for safety and security. Controlling access to postal operations and assets is as essential for co-locators as for postal employees; and in some cases, more so because of the inability to influence hiring or screening practices for other firms. Access controls, identification badges, and parking controls must be adhered to. If possible, it is best to deal with these issues before sharing space with outsiders, during rental or leasing negotiations, for example.

While it is usual to think of the neighbourhood a facility resides in as a primary source of threat, there is also potential security support to be gained by communication and cooperation with neighbours towards the mutual goal of safety, security and crime prevention. Meetings with community leaders can pay dividends in mutual support and cooperation. “Open house” invitations to facilities can create good intentions and transparency. Supporting or helping to develop “neighbourhood-watch-type” programmes or other cooperative efforts can help Posts be good neighbours and gain the eyes and ears of the community to assist in maintaining good security and crime prevention. The more Posts can help to make communities safer, the less threat they will have to deal with and the more secure their operations and employees will be. This can also help postal managers earn and create a positive business reputation.

The establishment of partnerships with other business entities, such as banking institutions, security institutions, airport authorities, business forums, consumer protection services and security service providers, can be beneficial in sharing ideas and concerns as well as providing mutual support. At the international level, coordination with other postal operators within the UPU and the PSG will enhance efforts to prevent crime internationally. Appropriate government and law enforcement agencies and prosecutors are also essential allies and partners in the fight against postal-related crime.

12 Law enforcement

Among the most important allies in crime prevention and response are partners in law enforcement. Substantial benefits can be achieved through regular interactions with prosecutors and other police officials to educate them on postal issues and concerns. In addition, postal security officials can provide training and consultation with law enforcement agents and prosecutors to assist them in understanding the unique issues of postal crime.

As discussed earlier in the section on the techniques and principles of risk assessment, police agencies can be a valuable source of crime statistics and analyses regarding threats and risks in certain locations and on various types of postal crime. In neighbourhoods with greater police presence, those officers have unmatchable knowledge regarding local crime, including prevention issues and challenges. By working cooperatively and drawing on that resource, Posts will gain a better understanding of postal security problems and opportunities.

Police response to alarms and attacks on postal facilities can be enhanced through liaison efforts and better understanding. Moreover, Posts can aid responding officers by being good partners in developing contingency plans for incidents such as violence, robberies, explosions, fires, burglaries and mail bombs. Posts can share intelligence with law enforcement relating to postal crimes, such as mail fraud, drugs in the mail, money laundering, pornography, stamp counterfeiting, etc.

Postal security managers can also be a valuable partner and resource for prosecutors and legislators by helping to draft postal statutes, laws and regulations that effectively deal with specific crime concerns. Postal security professionals can provide training and support to prosecutors in helping them prepare for trial or address complex postal issues that may come up during trials, as well as providing testimony. Security officials are often the first authorities to respond to a criminal attack or incident at a postal facility and play an essential role in crime scene and evidence protection. Their initial observations and interviews (if called for) are invaluable to prosecutors in successfully prosecuting cases.

It is in dealing with law enforcement and prosecutors that a Post’s integrity and professionalism is most crucial. Criminal matters require the highest degree of confidentiality, attention to privacy issues, and fairness. The benefits of criminal prosecution for postal matters can be most useful in reinforcing prevention standards for employees when processes are conducted with the utmost professionalism and fairness.

13 Misuse of Posts

In addition to providing security for facilities, and for people who are within those facilities, an important and sometimes more complex challenge for security officers is preventing the misuse of Posts. Misuse can result in harm to customers and employees and can erode confidence in the postal system. An effective prevention programme must also address concerns such as bombs and harmful items in the mail, the use of the mail for shipping drugs, money laundering proceeds, pornography, and fraudulent misrepresentations. Moreover, revenue protection risks such as fraud against Posts, stamp counterfeiting, cheque washing, theft and destruction, and meter fraud require attention.

A good prevention approach to these challenges can be enhanced through employee and customer awareness with training, brochures, information posters, and other multimedia resources. An important focus of this effort should be helping employees and customers be the eyes and ears of the first line of prevention. With this awareness, they can recognize irregularities and misrepresentations and know how to report their observations and concerns to appropriate authorities. Profiling of problem areas can be an invaluable tool for focusing attention on the most useful and productive areas. Along with being able to identify potential bomb or drug parcels, employees and customers should also know when to contact authorities and managers. A reward programme can be a way of increasing employee and customer awareness and involvement.

Sampling, profiling and survey techniques can be useful in identifying false and counterfeit postage and meter misuse. With regard to meter and postage misuse, working with meter and mailing industry representatives in a collaborative approach can be beneficial in identifying and eliminating risks of major loss. Large potential threats such as these are also excellent areas for PSG focus and attention. Other fraud against Posts, such as contracting, billing and procurement frauds, can be reduced through a programme of audits and best procedures.

Lastly, robust attention to misuse of Posts in the form of good policing and prosecution is a strong deterrent. Publicizing arrests, prosecutions, and the potential penalties for mail and postal offences can be very effective. Knowing that there is a good chance of being caught and facing a serious penalty can dissuade would-be violators from evading postal laws.

14 Security and investigative services

There are various ways of approaching and achieving prevention goals to ensure the continuity of postal operations and the safety of employees and customers. Senior managers, most likely with the involvement of security specialists, must decide whether the best strategy is to utilize internal security personnel resources and expertise, or to use external resources and hire contract security services. Likewise, depending on the flexibility of the postal environment, decisions must be made on the preference between internal and external investigative services or on strict reliance on regular law enforcement.

In evaluating the options, it is necessary to assess the many arguments for and against an internal or external approach. Cost versus benefit is certainly a major consideration for deciding on resources; but so are questions relating to expertise, motivation, loyalty, effectiveness, control, and level of attention to postal problems. Legal, enforcement and regulatory issues must also be addressed.

Whether internal security resources, external contracted services, or a combination of both are used, management must carefully evaluate the following high-priority areas and possible liability for the organization. Background investigations of security officials (internal or contracted) must be thorough and updated at reasonable intervals. Entry-level training and refresher training must be high quality, and need to deal with real-world issues and problems. Policies with regard to the authority of the officers – such as the use of force and whether or not to arm them – are sensitive subjects and must be clearly defined. Policies should also be frequently reinforced with training and review. The officers' official dress code is less critical, but is still important for the way security services are viewed by the officers themselves, as well as by employees and customers. There are both advantages and disadvantages to the use of uniforms, badges, and more casual clothing, with the decision taken having an important influence on authority and perception.

As mentioned, cost is not the only issue. Senior managers and those responsible for security programmes must also evaluate benefits and risks, which if not addressed wisely can result in greater future costs in terms of lost revenue, resources, morale, reputation, and customer/public support. The benefit of reducing or eliminating such future liabilities is the most important value of a good security programme. The relatively minor cost to today's bottom line can save tomorrow's revenues and preserve the organization and its employees.

15 Summary and conclusions

In summary, this document is intended to provide an overview of the many facets of an effective and comprehensive crime prevention programme. It has provided general guidelines in the areas of risk assessment (including techniques and principles), building and facility security, protection of equipment, technology, mail, finances, employees, customers, and others. General problems of misuse of postal systems may lead to professional interactions with law enforcement, prosecutors, and security and investigative services.

The intention has been to provide a holistic approach to security and crime prevention, which includes involvement of security professionals, management at all levels, employees and their representatives, customers, community groups, business associates, and others with whom Posts come into contact in the performance of their duties. As in all professional efforts, the more involvement and support received from those we work with and for, the better the chances of success.

This document does not have the answers to all of the complex issues and problems that can be associated with crime prevention; nor does it provide any suggestion of a perfect strategy. Criminal and security problems and breakdowns will always be part of security specialists' ongoing challenge. The lessons of cooperation, participation, flexibility, assessment and analysis, combined with experience-based creative thinking from security specialists and managers, provides the best hope for success in staying a step or two ahead of those who would harm postal facilities, employees and customers.

This document provides a broad-based checklist of issues, concerns and approaches for security professionals. Using these guidelines, ideas and approaches, those with important security responsibilities can formulate strategies to address specific problems and challenges that can arise in the complex world of postal security and crime prevention. The possibilities for differing available strategies are as numerous as the possible forms of criminal attack.

An example of a useful strategy, developed by the Security and Investigation Services of the South African Post Office, is provided in the appendix, entitled “Problem solving as a crime prevention strategy”. This phased approach involves methods of identifying the problem, problem analysis, response, evaluation, and action planning. This model of effective problem solving is provided as an example of how security managers can address security concerns and, through a thorough, logical and comprehensive plan, address prevention concerns and challenges.

Special appreciation is extended to the Security and Investigation Services of the South African Post Office for providing this model and for their pioneering work and ideas in developing these guidelines. Without their excellent effort, this document could not have been produced.

Appendix A

Problem solving as a crime prevention strategy

Officials within the Security and Investigation Services deal with an exceptional number of problematic situations. Theft of mail, robberies at post offices, postal bank fraud, mail violations, credit card fraud, and theft of cash and stocks are a few examples that occur almost daily. Tampering with mail at mail centres and the exploitation of the postal service for drug trafficking are ongoing issues, despite follow-up investigations and imprisonment of perpetrators.

Traditionally, it was believed that the only way to reduce these incidents was to investigate and address individual incidents. The number of suspects charged, suspended or discharged measured the success of dealing with incidents. When incidents appeared to be under control, a search began for the next incident to investigate, suspend and detain again. This incident-driven strategy:

– displays a reactive rather than a preventative approach;

– relies on limited information collected from victims, witnesses and suspects; and

– necessitates an appeal to the justice system to deal effectively with all incidents.

Too often responses are ineffective, time consuming, and show few tangible results. Frequent reoccurrence of similar incidents shows that an incident-driven approach is unable to address the underlying circumstances.

The theory of problem solving is based on the premise that underlying circumstances cause the problems. These circumstances may include:

– Physical surroundings which might create opportunities for theft or robbery;

– Flaws in systems that can create opportunities for fraud and theft which can be very difficult to detect; and

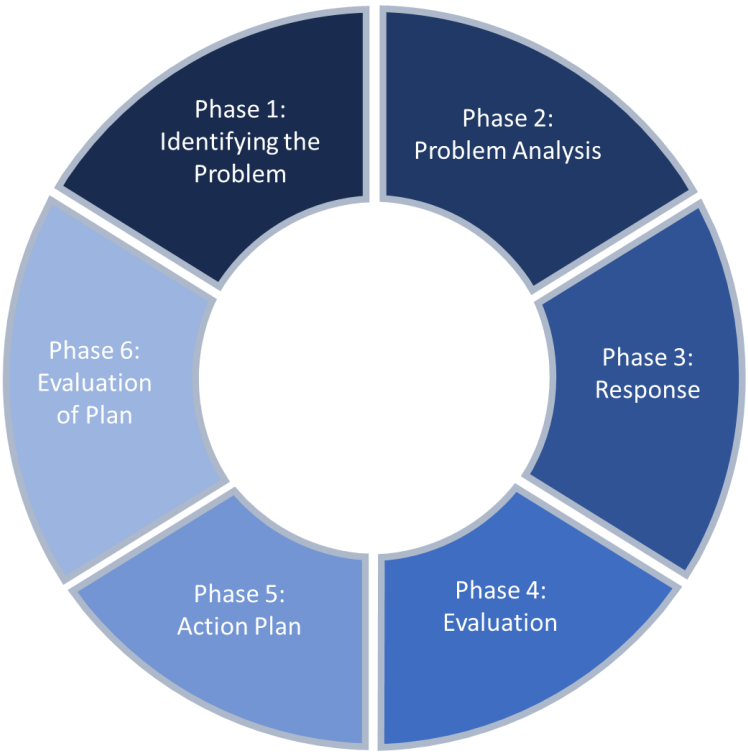
– A lack of effective management or supervision which can lead to various unacceptable behaviours and can result in various crime-related incidents.

These incidents, although they have a common cause, are only symptoms: as long as the underlying problems exist, incidents will continue to occur.

Problem solving focuses on the causes of incidents – how to deal with them. This focus establishes an effective balance between reactive and proactive approaches to security.

Through the formal introduction and acceptance of problem solving, the problem-solving process becomes a generally acceptable and acknowledged activity that forms part of daily operations.

Problem-solving model



Phase 1: Identifying the problem

In the analysis of a problem, e.g. theft of mail, robbery, etc., a detailed analysis should preferably be carried out as thoroughly as possible. The specific facility, type of property, time of occurrence, modus operandi, etc. may all point to different problems, each requiring a different solution.

1 Defining a problem

A problem constitutes a series of related and/or repeated incidents. Characteristics that show repeated occurrences or connection of incidents are the following:

– *Behaviour*: The occurrence of common behaviour is probably the easiest way to identify the number of incidents as a problem. This is especially true when concentrating on city-wide or national problems such as theft of mail, robbery at post offices, and fraudulent postal orders;

– *Area*: A collection of different behavioural problems within a specific area can result in problems being identified according to the place where they occur, for example the tampering and theft of mail at major mail sorting areas;

– *Time*: The repeated occurrence of incidents can be defined as a problem according to their repetition at a specific time, season, day of the week, e.g. tampering with mail during the tax season, robbery at post offices at closing time, theft of cash at the end of month;

– *People*: A problem may be identified in terms of offenders and/or victims, e.g. syndicates, cashiers, etc.

2 Identifying problems

The identification of problems requires:

– Input from everyone in service roles within the Post, from administrative clerks to guards, cashiers and general staff, etc.;

– Serious consideration of information reported by customers;

– Consideration of recommendations made by organized groups, e.g. community police forums, business, federal agencies, labour unions;

– Customer inquiries;

– Compensation payments;

– Analysis of the large number of incidents conscientiously recorded by the Security and Investigation Services.

The media is generally seen as the voice of the community. A study of media reports may indicate that a particular community or group of people has negative perceptions of a specific problem with the Post or in relation to the service it renders, e.g. corruption.

Various other potential sources can be utilized to obtain information for problem identification. These include data from service calls, written complaints, calls for help, police statistics, etc. The Security and Investigation Services of each region should identify local information sources in order to utilize all available information.

3 Prioritizing problems

The problem-identification process will inevitably identify more problems to be dealt with. The limited availability of resources necessitates the prioritizing of identified problems. National or regional problems require intensive analysis, which may be time consuming. The security and investigation services official may possibly be confronted with a series of problems of varying complexity and extent. This means that selection criteria must be determined. The following factors may be considered:

– The presence of any life-threatening circumstances;

– Customer interest in solving the problem;

– The likelihood of resolving the problem – to what extent do the security and investigation services have the ability to resolve the problem;

– The seriousness of the problem – how much danger, scandal, public interest does it reflect;

– The consequences for the Post – harm, damage and loss.

Phase 2: Problem analysis

Examine the problem (the five Ws)

The next step is to investigate the problem by dissecting it and identifying all elements of the problem.

During analysis, it is very important to consider the five Ws. The questions to be answered are: *Who? What? When? Where?* and *Why?*

Consider information about the victim, offender and situation – When analyzing the problem, be sure to gather sufficient information on the victim, offender and situation to assist in developing strategy responses in the next step. The situation includes circumstances that contribute to the problem as well as environmental factors that may affect it (e.g. lighting conditions, geographical factors, and weather/climate considerations).

Consider information on the victim, offender and situation by examining the problem through each of the following factors:

– *Impact*
  - How significant is the problem?
  - Who is affected?
  - What other problems are impacted by the situation?
  - Who are the stakeholders?

– *Seriousness*
  - What is the impact if left unchecked?
  - What is the public concern or perception?
  - What is the police priority/status of the case?

– *Complexity*
  - How complex or deep-rooted is the problem?
  - Are resources available to handle it effectively?
  - Who has ownership?
– *Solvability*
  - To what extent can individuals, teams and/or the community impact the problem?
  - If not, what is required?
  - What is the cost?

Methods of analysis

The following are some methods you may decide to use for analysis of the problem:

– Informants
– Incident analysis
– Direct observation/surveillance
– Focus groups
– Interviews
– Research at libraries/via the Internet
– Meeting with other agencies
– Surveys, questionnaires

Note. – Do not be surprised if, during analysis, you need to redefine the problem. You may also find that you have more than one problem.

Before considering strategy responses, clearly define the problem. Now that you have identified the problem, the goal must be established. The goal must represent one of the following intentions:

– *Eliminate the problem*: Usually these are small, simple problems involving few resources with minimum costs.
– *Reduce the problem*: Persistent, deep-rooted problems that cannot be eliminated entirely.
– *Reduce the harm or impact*: If a problem is difficult to reduce or eliminate, security teams may be able to reduce its impact upon victims, the Post and/or its reputation.
– *Redefine the problem responsibility*: The team must look at ways of returning misplaced responsibility that generates inappropriate workloads for the Security and Investigation Services. It must be recognized that security and investigation officials are not exclusively responsible for all crime-related postal problems, e.g. robberies, vehicle theft, etc.

Decisions on the above goals will focus the Post's strategies in certain areas.

The challenge is to develop appropriate responses for these problems at the local level. There is no single cause for crime-related problems, because different types of crime have different root causes and hence require different approaches to prevention.

Phase 3: Response

The choice of possible responses (solutions) is only limited by the imagination. Creative thinking and a broader approach to problem solving are the keys to success. Problem-solving strategies should be aimed at specific problems. For example, strategies developed for general theft would be more effective if developed for a specific theft problem.

Note. – Problem solving must be based on a commitment to develop a specific response for a specific problem in a specific location under specific circumstances.

From analysis of the problem, reactive and proactive responses will be developed by the security and investigation services management and relevant stakeholders, e.g. unions, police agencies, etc. Many of these stakeholders have formed traditional responses, which will likely continue to be identified as effective strategies to address problems.

Phase 4: Evaluation

The objective of problem solving is to successfully address a specific problem. Therefore, it is essential that methods of evaluation be developed to gauge the impact of security strategies on the identified problems. No organization can afford to utilize valuable resources without a definite indication that it is cost-effective. Unconfirmed opinions that the approach is working are no longer sufficient. This means that:

– Some method of proof or at least evidence that a specific strategy is effective must be submitted. The increase/reduction in or continuous occurrence of the problem, financial saving/losses for the Post, damages prevented, and the recovery of assets and value thereof are a few factors that should be considered when determining the evaluation criteria;

– The formation of clearly measurable goals will establish explicit standards;

– A clear understanding of the problem must be presented.

Phase 5: The action plan

– *Team*: Identify the team with ownership of the plan;

– *Problem/issue*: State the focus of the plan;

– *Goal*: State the goal of the plan (to eliminate/reduce…);

– *Strategy*: The strategy should be specific to the following criteria: what is to be done to accomplish objectives of the strategy?

– *Task*: List the specific task to be accomplished:
  - Who?
  - Where?
  - Completed when?

Note. – Tasks related to monitoring and evaluation of the strategy should also be assigned.

– *Activity*: Statement of results by the individual completing the task.
  - Who?
  - Where?
  - When?
  - What result?

– *Strategy*:
  - Results (anticipated and unanticipated)
  - Consideration of best strategy or other learning results

– *Action plan results and evaluation*: Indicate the results of the plan and the evaluation methods used to determine success.
  - Were you successful?
  - How do you know? (results of evaluations)
  - What strategies did or did not work?
  - Were there any unanticipated results?

Phase 6: Evaluation of plan

Complicated analysis is not required to determine whether or not you have been successful in meeting the objectives. For example, if your goal was to eliminate or reduce a problem, these measures will be largely quantifiable (e.g. mail fraud complaints decreased 45% over the last six months). Crime and occurrence statistics will indicate whether or not you were able to make a difference.

If, on the other hand, the goal was to reduce the harm or impact, the measure used might need to be more qualitative in nature (e.g. responses to a victim's survey indicating increased satisfaction with a service received).

Problem solving requires that each security and investigation services official will search for solutions to the problems confronted every day. Approaches and instruments must always determine whether they are morally and legally justifiable. The approach or instrument must also be critically analyzed in respect of the success that can be achieved with it.

Without intending to restrict thought or creativity, the following are a few options that could be applied in addressing identified problems:

– *Enforcement response/investigation* – The application of enforcement/investigative strategies, whether random or directed, towards identified problems or issues.

– *Police/law/regulations* – Implementing/adopting new policy, establishing new procedures and adopting the use of broader public laws.

– *Mediation/negotiation* – Negotiation as a way to resolve conflicts, which can be particularly useful in common situations where there may be no single correct solution. Negotiation refers to a process where conflicting parties talk to each other to attain a mutually acceptable solution.

– *Communication strategy* – A communication strategy can be used to reduce fear of crime and victimization.

– *Enabling postal officials to help themselves* – Address and resolve uncertainties regarding laws, policies or procedures; warn potential victims and advise them on security precautions; make postal employees aware of possible criminal activities; and gain support for a solution/programme, etc. Communication media such as e-mail, radio, television, pamphlets and newsletters can be used in anti-crime campaigns. A creative search can offer new possibilities, such as workshops.

– *Mobilizing all employees* – Mobilization refers to efforts to involve all postal employees and interested groups, such as trade unions, as a whole or separately, to address crime in general and solve problems.

– *Environmental design* – Consideration of environmental issues that might contribute towards a problem/issue, including factors such as roadways, parks, parking lots, the placement of shrubs, street lighting, etc. This can be an issue for immediate response to an identified concern.

– *Interagency/stakeholders* – Formal and informal mechanisms for working with agencies, institutions or other stakeholders which are involved in and have "ownership" of similar problems. May range from simple referrals to working in partnership.

– *Targeted crime prevention* – With targeted crime prevention, the significance and effort related to committing certain crimes is increased by reducing the profits of the perpetrator as a result of managing, designing and manipulating factors in the physical environment. This can be achieved by establishing measures aimed at the reduction of opportunities for committing crime and is done in the belief that it will deter criminals or at least result in the transference of crime.

– *Target hardening* – Target hardening refers to any physical hindrance that is placed in the way of a prospective criminal to increase the difficulty of committing a crime. Such obstacles should contribute to the identification of criminal behaviour and the arrest of the criminal. Examples of target hardening include: counter screens in post offices; protection of valuable articles in safes; burglar bars; reinforced doors; and alarm systems.

– *Access control* – Access control aims at limiting or preventing access to a specific locality (building or terrain) or system (for example computer systems). Access control can be implemented by: the erection of fences, walls, gates and motorized gates; the use of intercom systems and access cards; reliance on guards, receptionists and porters; and the use of passwords and identification codes.

A crime prevention strategy can only be successful if practical and as part of a project-driven process to solving problematic environments.