



## **From Incident Reports to CPTED Initiatives: Using Internet Reporting and Analysis**

*Alana Pickels and Susan Urosevic  
Amtac Professional Services  
Brisbane, Australia*

### **Introduction**

Contemporary technology has had a significant role in the monitoring and analysis of crime. The use of such technology to aid in the implementation of crime prevention strategies has been identified as an effective method of reducing crime. However, in order to develop effective crime prevention strategies, it is essential to first understand the specific nature of incidents. One of the most commonly used techniques used to gather incident related information is an incident report. These reports can vary greatly in format depending on the type and quality of information that is being recorded, how it will be used and for who the information is being gathered. One typical error within organisations is the use of incident report forms that are not specifically customised for the organisation.

This paper presents a discussion of incident reporting and the use of technology to improve data analysis and aid in the implementation of crime prevention strategies. The potential to tailor incident reporting systems to individual organisational contexts will also be explored. It is essential that organisations utilise incident report information to make informed and reliable security risk management decisions. For this purpose incident reports need to be concise, easily accessible and should be customised to reduce the opportunity for misinterpretation of data.

### **Online Reporting**

Amtac Professional Services (“Amtac”) has developed the technology to assist clients with the reporting of security and safety incidents. Amtac’s online incident reporting system is flexible and may be customised to meet the needs of individual clients. This paper will further discuss the potential to utilise incident reporting data to identify crime patterns and safety issues that may otherwise go unrecognised. This data, in combination with onsite evaluations, can subsequently assist management in the application of CPTED strategies to reduce identified crime and safety issues.

The ability to make informed and reliable security risk management decisions from accurate data is directly correlated to the quality of information collected. In broad terms, comprehensive statistics drawn from incident report data may be used by numerous stakeholders including police, legislators, city planners, and external organisations. As incident data is often used by numerous stakeholders, it is extremely important to have reliable and consistent terminology. It is critical that all security and safety related incidents are recorded, so that site specific vulnerabilities and the frequency of these incidents can be identified. However, it is essential to first educate those responsible for reporting incidents.

Staff awareness plays a vital role in the amount and type of incidents that are reported. Traditional incident reports which require a hand written, narrative explanation of

---



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

events may be difficult to read, subject to interpretation or may not contain sufficient details. This presents difficulties when attempting to analyse the data. Similarly, factors such as literacy levels can affect the quality of incident details that are collected. A review of a major public transport client within Australia found that staff were required to hand write an incident report at the completion of a long shift. However, difficulties arose due to low levels of staff literacy within the organisation. This combined with the personal time required to complete an incident report significantly affected the quality of information being recorded. Subsequently, many incidents were not reported due to inconvenience and difficulties imposed on staff members.

Practical experience suggests that a significant portion of security related incidents are not reported within many organisations. In addition to the above, incident reporting deficiencies may also occur due to influential factors such as staff perceptions and tolerance levels, attitudes towards management and the police (Taylor, 2002). Research suggests that there is a far greater chance that incident reports will be completed when there is evidence of a crime being completed or insurance claims are involved (Taylor, 2002).

Incident reports do not necessarily require staff to complete a hand written narrative report. Drivers within the above mentioned public transport organisation should be encouraged to report all security and safety related incidents no matter how trivial. An initiative implemented by Amtac included the introduction of radio based incident reports. Through simplifying the reporting process, incidents that would have previously been tolerated or ignored and not reported are now reported via radio, providing more accurate information for analysis. Changes in procedure, in addition to staff training, encouraged staff within this organisation to become more aware of the reporting process and understand the reasons for reporting all incidents, no matter how trivial. Similarly, when users understand the reasons for reporting and recording an incident they are more likely to include supplementary relevant information. Notwithstanding the above, supplementary information must also fit into uniform classification systems to assist in its analysis.

At present numerous organisations use various forms of software to record security and safety related incidents. Software, such as the Incident Reporting and Investigation Management System (IRIMS), can be programmed to record specific categories of information. As with most information systems, there can be numerous positives and/or negatives associated with usage. Geographic Information Systems (GIS) are an extremely useful tool that may be used to identify crime hot spots, and further analyse the spatial patterns associated with crime and offender behaviour.

However, both of the above systems make a number of assumptions about the competencies of users. Technological competency and literacy levels can greatly influence how effectively the system is used. Additionally, the use of such reporting systems can also become resource intensive. Within some organisations one individual fills out an incident report, which is then passed on to management or security, were a second individual inputs the information into the incident reporting

---



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

system. This process is not only time consuming but also affords the opportunity for error as information to be re-entered may be misinterpreted, lost or distorted.

### **Information Dissemination**

Amtac has developed the technology to assist clients with the reporting of security and safety incidents. Systems employed by Amtac are extremely flexible and may be customised to meet the needs of individual organisations. Amtac has delivered an online incident reporting system or a palm pilot based incident reporting system for onsite inspections. Incident data collected via the palm pilot can later be uploaded onto the online reporting system. At present the most popular form of incident reporting used by Amtac clients is the online incident reporting system. When an incident occurs, users are able to log into the internet and complete an incident report. The process of entering information into the system is structured, rather than allowing the reporter to write a narrative explanation. Once the user enters a unique login and password, they are required to complete a series of questions relating to the incident.

The questions have also been tailored to suit the needs of external third parties, such as police, insurance agencies or maintenance contractors, who may also require access to the report. Once the initial details of the incident have been registered on the system, selected stakeholders are notified and incident details are available for authorised third parties to access. If additional information regarding the incident becomes available it can also be added to the report at a later date. System users have a controlled facility to search, display and update a summary of incidents, commensurate with their authorised level of access. Amtac's incident reporting system also has the ability to produce structured reports from the collected incident report details.

Due to the sensitive nature of information that is being recorded various security measures are in place in order to make the system resistant to compromise. The incident reporting system can be accessed via the internet on a secure link Secure Sockets Layer ("SSL") encryption of data. As it is recognised that the data from the system is a critical resource, appropriate actions are taken to ensure that it is not compromised. On another level, users of the system must provide sufficient personal information in order to register for access to site specific areas of the system.

### **Crime Mapping**

The type and quality of information that is being recorded depends greatly on the purpose for which the client requires the data. Another system that Amtac has been involved with incorporated concepts of crime mapping into its security and safety reporting system. Visual representation of crime patterns through computer generated maps, offers an invaluable opportunity for focusing resources in more efficient and effective ways. Incident reporting systems that incorporate crime mapping afford clients the opportunity to develop a greater understanding of their crime and safety issues.

When a client incorporates crime mapping into their incident reporting system, areas of the property are divided into zones so that specific locations can be accurately identified. This allows the exact location of incidents to be monitored more closely

---



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

than if they were recorded in a narrative format. For example a bush on the western side of the perimeter may only be identified as such in a narrative sense, however if the area has been divided into a grid pattern the exact location is more easily identified, and in turn more effective crime prevention strategies can be developed for that location.

The use of statistical information generated through incident reports provides an invaluable tool for crime prevention initiatives. The information base that is generated allows a qualified analyst to uncover incident patterns and relationships between the situational factors surrounding individual incidents. Crime Prevention Through Environmental Design (CPTED) is a branch of situational crime prevention and states that the physical environment can be changed or managed to produce behavioural effects that will reduce the incidence and fear of crime (Crowe, 1991). CPTED strategies use the principle that the design of the environment may be modified to remove facilitators of crime and to affect the perceptions of users within a given space – addressing not only the opportunity for crime but also perceptions of fear on the part of those who may otherwise be victims.

### **Enhancing CPTED through Reports**

Amtac recognises that there is great potential to further develop CPTED-based initiatives from both its current online incident reporting system and on site security surveys. A number of clients currently utilising the system regularly access statistical information regarding incidents that have been entered. Based on the user requirements, customised reports can be extracted and emailed to various stakeholders within the organisation. The reporting facility provides information relating to the frequency and type of incidents that have occurred on a specific site or within a specific area. Technology allows for specific reports to be deployed in predefined circumstances. For example, when two similar incidents occur within a specific geographic area stakeholders are automatically emailed a report. The format in which this report is communicated may also vary. In addition to an email, the system has the capacity to send a text message to an authorised mobile phone.

In practice, CPTED principles can be, and are, used in a wide range of contexts, from social planning through to urban design; from community safety to specific security risk management applications. Whilst the underlying principles can be traced back to ancient civilisations, contemporary concepts of CPTED have been around for forty years or so and may be applied to numerous professional disciplines such as architecture (Department of Education and Training, 2002). Yet there remains a high degree of CPTED illiteracy within the professions, frequently resulting in designs that fail to fully meet behavioural or functional objectives. The by-products of which are fear, reduced productivity, and increased opportunity for crime (DET, 2002).

It is recognised that CPTED principles can be of substantial benefit when developing integrated security solutions. Specifically, it can be used to develop site-specific security measures that aim to reduce opportunities for specific incidents to occur. Amtac has in the past tailored its reporting system to gather information specifically related to robbery risk assessments. During this project one hundred and twenty-four (124) sites were examined. Preliminary research involved analysing information

---



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

including, but not limited to, site plans, floor plans of all buildings containing cash handling facilities, documented policies and procedures, and scheduled hours of use of buildings and grounds. In addition to the background information, Amtac staff undertook site visits which incorporated formal and informal interviews, examinations of the built environment with particular attention to identifying deficiencies. Information for this project was gathered with the use of Palm Pilots and digital camera's. Whilst on site Amtac staff members completed a standard survey, specific to the project. This survey focused on specifics such as opening hours/closing hours, the number of staff within the cash handling facility, the levels of cash held within the location and environmental design features. Environmental factors included the proximity of the cashier to exit/entry points, the height of the cashier counter, and the ease with which the counter may be breached. This information was all collated into a single database which formed the basis for recommendations which had a CPTED focus.

### **CPTED in Educational Facilities**

Educational facilities are an area where the application of CPTED strategies can provide tremendous benefit. Amtac has worked with numerous educational organisations to develop strategies and implement CPTED initiatives. There is a need for all staff and contractors to take reasonable steps to identify, assess and manage the safety and security risks related to their areas of responsibility. The development of a central incident reporting system provides the basis for coordinated strategies. In order to ensure the effectiveness of any strategy all aspects of security risk management must be integrated into the overall management within each site. Good planning should also include pro-active and reactive elements in order to effectively manage unforeseen risks or vulnerabilities (DET, 2002).

Additionally, early intervention practices aid in minimising the consequences should an unexpected event occur. It is important to also reflect on the intangible elements as well as economic costs that a security or safety incident may incur. Consequences of a security or safety incident are often measured in economic values, however, reputation or lives can not be appreciated in monetary values. Through the conceptualisation of the consequences of all risks, organisations can develop a clearer understanding of risks in context, and this provides for more effective risk management decisions.

Within educational organisations, security is considered to imply a stable, relatively predictable environment in which staff and students may pursue teaching and learning without disruption or harm, or without fear of disturbance or injury (DET, 2002). From this it is important to realise that school security management must include a range of strategies to protect not only people and property, but also activities and the reputation of the school. It is also important to realise that there are a variety of ways in which educational facilities may be placed at risk. People may be assaulted by individuals from within or outside the educational facility. Property such as information may be compromised, lost, stolen or vandalised. School activities such as lessons may be interrupted or cancelled, and damage to school reputation may effect

---



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

its attractiveness to staff, students, and/or the community which in turn could reduce its capacity to raise funds.

It is essential to note that if and when a security or safety incident does occur, it should be reported as soon as possible after the fact. One of the most important tools for effective risk management is the collection of reliable and accurate incident data. It is therefore important to record all relevant information while it is fresh in the minds of those involved. Subsequent to any incident it is important to review both the incident and any strategies that may be applied in order to more effectively manage incidents. This is where CPTED initiatives can often be effectively introduced. Although it is essential to exercise caution in the extrapolation of CPTED initiatives from individual experiences, it is also important to recognise the effectiveness of site specific CPTED strategies. Through applying commonsense CPTED principles to educational facilities there is an opportunity to reduce security risks that are faced on a daily basis. Some basic recommendations that are encouraged include the use of signage - to identify buildings within the facility and remove excuses for unauthorised access, locating gathering areas in locations with good natural surveillance and the use of the vegetation to ensure that landscaping does not inhibit opportunities for natural surveillance (DET, 2002). Further recommendations include avoiding the use of rocks or loose pavers that may be used for injury or vandalism, securing rubbish bins at the end of each day, and minimising the number of entry points into the campus (DET, 2002). CPTED principles that are generally recommended are typically a common sense approach to crime prevention which may be implemented immediately with relatively little cost.

### **Conclusion**

There is great value in developing customised incident reporting systems. Tailoring incident reporting systems to the specific needs of organisations allows for more comprehensive information to be gathered. Subsequent analysis of such data allows organisations to make more informed and reliable security risk management decisions. The importance of staff training and understanding of the incident reporting system is essential in gathering specific incident information.

In gathering accurate incident reports, there is greater potential for targeted CPTED initiatives to be developed and implemented. Through the co-ordination of management and the implementation of both general and site specific CPTED strategies there is great potential to reduce crime and antisocial behaviours within many organisational settings.

### **References**

Crowe, T. D. (1991). *Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts*. Boston: Butterworth-Heinemann.

Department of Education and Training (2002). *South Australian Schools Security Risk Management Manual: Maintaining welcoming, safer and more secure campus environments*. Adelaide: Department of Education and Training.



*Proceedings of the 9<sup>th</sup> Annual  
International CPTED Conference 13-16 September 2004*

---

Taylor, N. (2002). Reporting of Crime against Small Retail Businesses. *Trends and Issues in Crime and Criminal Justice* Number 242. Canberra: Australian Institute of Criminology.