

Security Solutions for ATM's

by

Karim H. Vellani, CPP, CSC

And

Mark Batterson, CPP, CSC



(281) 494-1515
kv@threatanalysis.com
www.threatanalysis.com

Banks have been robbery targets as long as they have been in existence. With bank management comes specific crime prevention standards and most bank managers are well-versed with these standards. The primary focus of this article is on crimes occurring at Automated Teller Machines (ATMs) where quick cash is the prime target for criminals rather than at banks themselves.

Crime at ATM's has become a nationwide issue that faces not only customers, but also bank operators. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers.

In general, the United States banking industry has recognized the threat that ATM machines pose to the banking public. In effect, customers are often locked out of the safety of the bank lobby, and, therefore, totally subjected to the security preparations or lack thereof, dictated by bank management. Additionally, the banking public is lulled into a false sense of security when utilizing ATM's. After all, banks often go out of their way to exude a sense of stability, confidence, and security in the bank lobby. The subtle message: your money is secure and so are you!

To illustrate the banking industry's understanding of the dangers posed to ATM customers, the American Banker's Association and the Bank Administration Institute launched a victimization study of ATM-related crime. This study was in response to proposed Federal legislation that would mandate nationwide minimum requirements for ATM locations to include such minimum standards as: alarm systems, surveillance cameras, secure enclosures, and ATM crime prevention education programs for customers. In an article published in a prominent banking industry journal, the following list of recommendations was contributed by industry experts to improve customer safety while utilizing ATM devices:

- Determining the crime risk in the geographical surroundings
- Locating new ATM's in highly visible areas
- Providing sufficient lighting at and around the ATM's
- Educate customers periodically by mailing a notice advising of risks associated with using the ATM and how to avoid these risks

- Maintaining shrubbery and other environmental features at a height at which they cannot be used for concealment
- Conducting and documenting periodic security surveys at the ATM location, and sharing that information with local law enforcement officials
- Providing a direct-line phone to a bank department so that customers can call for assistance around the clock
- Educating bank personnel to be responsive and sensitive to customer claims and to communicate such claims immediately to bank security.

Further illustrating the point are recent ATM security laws that are being enacted in various jurisdictions across the country. For example, in 1993, the city of Chicago appointed an advisory committee to consider the adoption of an ordinance that would mandate certain minimum safety provisions concerning Automated Teller Machines.

The commission recommended that banks need to evaluate the safety at ATMs which are exposed to the street or located in a building. Recommendations included adequate lighting, evaluating visual obstructions around ATM's and the evaluation of incidences of crime in the vicinity of the ATM's as reflected in records of local law enforcement agencies and the institution's own internal records.

In 1996, Illinois enacted The Automated Teller Machine Act. Section 20 of the Act provides procedures for evaluating the safety of ATM's regarding "the incidence of crimes of violence in the immediate neighborhood of the ATM."

Although Illinois seems to be at the forefront of ATM safety legislation, other states are studying ATM safety issues and the US Congress is also getting in on the action. A bill (H.R. 3662) introduced by Representative Steve Rothman (D-NJ) would require the Federal Reserve System to adopt mandatory minimum requirements for the security of ATM users including:

(5) Other Preventative and Remedial Measures:

The standards shall require the security officer designated by any operator of an automated teller machine to take such other actions as the security officer may determine to be appropriate and useful to prevent crimes in the vicinity of the machine and to preserve evidence in the event of any such crime, taking into consideration the following:

- (i) *The incidence of crimes against consumers, including users of automated teller machines, in the vicinity of the automated teller machine.*

As this clearly illustrates, analyzing crime history and trends at ATM locations is rapidly evolving from "best practice" to federally mandated. Furthermore, criminal incidents are oftentimes foreseeable, and the likelihood of their occurrences would be greatly reduced through the implementation and follow through of basic ATM security procedures. Banks have a responsibility to exercise reasonable care in the protection of their ATM customers.

As seen in the above examples, analyzing crime at ATM's is becoming more than just an industry standard, it is becoming law in many parts of the country. Moreover, crime analysis is now recognized by the American Society of Industrial Security and professional security personnel in general to be a business best practice. With that in mind, we should define the term:

Crime analysis is the logical examination of crimes which have penetrated preventive measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants, as well as the application of revised security standards and preventive measures that, if adhered to and monitored, can be the panacea for a given crime dilemma.

Thus, crime analysis is not only required by law in certain jurisdictions and an industry best practice, but it is also the first step to creating an effective security program. As such, its objectives are many:

1. To reduce crime on the property.
2. To evaluate and aid in the selection of security and crime prevention measures.
3. To justify security and crime prevention expenditures.
4. To provide a system of monitoring the effectiveness of security and crime prevention measures.
5. To provide a continual evaluation system of the property's crime situation.
6. To reduce the liability of property owners and their agents (property managers and security companies).

Having outlined the objectives of crime analysis, we should take a look what crime analysis is and is not. Crime analysis is not demographic data that determines risk for an area using unknown data points and some far reaching social disorder theory, nor is it data from other unrecognized sources. To the contrary, crime analysis is based on actual crime data pulled from law enforcement databases. The difficult part here is accessing those databases from each and every police department where we have a bank or ATM.

Given that we now know that crime analysis uses actual crime data, we should define the methodology that is proven, is considered a best practice, and most important, is accepted in court. The first step is to obtain the police department data for each location. This data usually comes in the form of Calls for Service (CFS), which provides a 90% accurate portrayal of criminal and other activity at a property. With this initial data, we can begin to build our database of crimes at each bank and ATM. CFS consists of each call to the police to report crimes or other activity from the location.

Remember, we said that CFS is only 90% accurate. To get closer to 100% accuracy, we have to go one step further by obtaining the offense report for each incident that concern us. Offense reports are the written narrative of a call for service that resulted in an actual crime. With these in hand, we are able to understand the true nature of risk at our banks and ATM's.

Once we have our database of actual crimes built, we can begin to analyze the specific risk at each site. There are a number of queries that will assist in creating an effective security program. The first is a crime-specific analysis which focuses on the type of crimes committed on the property. Knowing what crimes have occurred will aid bank managers in knowing the specific crime problem, to what degree it exists, and indirectly what specific prevention measures should be implemented. It can also tell us what particular asset is being targeted and the resulting loss or damage to that particular target and the implications of that loss or damage.

The next one is a property-specific analysis which will help us differentiate between crime risks when comparing sites. For resource allocation, it is imperative that the analysis is focused at the property level. Given a security budget of \$100,000 per year, this analysis allows us to compare risks at each site and allocate accordingly.

Temporal Analysis is the third query. This analysis tells us when the risks are high and helps us efficiently allocate our security resources when threats are more likely. Various methods for learning a property's crime patterns can be considered including time of day, days of week, week of month, seasonal trends, and, on the extreme, crime trends during full moons. Temporal analysis is where bank managers will gain the highest return on investment.

You will find that crime analysis does not stop with these analyses and applications of security measures, but takes further steps to monitor the crime situation. Crime analysis continually monitors the crime picture, typically on an annual basis so we can test the program's effectiveness and revise if necessary. Crime analysis makes a static security program dynamic, providing for change.

The necessity to develop and maintain a well-balanced security program is elementary and essential to the protection of banking customers and other assets. Crucial to such a program are the balanced applications of crime analysis, security selection & implementation, and monitoring. In addition, potential liability can be avoided if management responds appropriately to the property's crime experience. Premise security cases are much less supportable if management conducts crime analysis, anticipates certain activity, and implements reasonable crime countermeasures.

Like most other tasks that bank and security managers must do, there are two solutions. The first is to hire, train and supervise a person or team of people to pull the data from each police department where we have a bank and ATM. The other option is to outsource this task. Since the new laws came into effect, many companies have begun offering this service. Outsourcing appears to be the most common alternative as it reduces costs substantially and brings third-party objectivity to the project. Also, the expertise to conduct crime analysis is somewhat limited given the high demand for it today.

Author Biography

Karim H. Vellani, CPP, CSC is a security consultant with Threat Analysis Group, LLC, an independent security consulting firm. He is a member of the International Association of Professional Security Consultants and ASIS-International. He is Board Certified in Security Management (CPP) and a Certified Independent Security Consultant (CSC). As a security consultant, Karim has extensive experience in risk and security management. He has authored two books, Applied Crime Analysis and Strategic Security Management: A Risk Assessment Guide for Decision Makers. Karim can be reached via email at kv@threatanalysis.com or via phone at (281) 494-1515.