



Risk Management Associates Electronic Newsletter

January 2009

Contents

- Introduction
- New Location
- New Logo
- 2008 Pinnacle Award
- Workplace Violence
- Terrorism in the United States
- Electrical Utilities



*RMA management team:
Back row: Michael Longmire, William (Bill) Booth, and Jerry Blanchard. Seated: Michael Tucker, Christine Peterson.*



Introduction

This is the inaugural edition of the RMA electronic newsletter. Many of you are clients, others of you are associates, and some of you are simply respected and valued friends of the company. In the past, RMA has distributed articles and items through email to many of you on topics that ran the gamut from workplace violence to biometric access control and from weather information to soft intelligence on terrorism. The majority of these distributions were directed to selected individuals along what we thought to be your lines of interest.

This practice will continue. We are, however, going to produce a general interest electronic magazine that will feature not only information about security interests in general, but information about RMA, our individual and collective experiences, and our opinions and insights about selected topics of general interest to the security community.

Our mission through this media will be to inform you about new things, discuss and refine old things and at times, provoke your thought and circumspection about specific things that are emerging in our mutual professional sphere.

To this end, we promise to live up to our core values of independent appraisal, unbiased assessment, and forthright analysis in our editorial selections, written articles and expressions of thought and opinion.

Thank you all for your past and current associations with us. We hope that through this newsletter, RMA can update and inform you, familiarize you with our company and staff, and solicit and establish a dialog about security issues with and among you.

The world around us is changing fast. The challenges in providing safe and secure environments for our companies and agencies are ever increasing. In some small way, we hope that our newsletter will provide assistance in meeting these challenges by purveying the collective information and experience gained during the many years we have worked in this field.

New Logo

The RMA management team has spent a lot of time and energy conferring with employees and clients about how the company could best evolve to meet the challenges and changes in our business. As a symbol of that evolution, it was decided to develop a new logo that represented RMA's new vision. Most of you are familiar with our square RMA logo which has served us well over the years it has been in use.

RMA is introducing a new logo that incorporates our pride in our past with our confidence in our future. It retains the familiar "RMA" script, along with a representation of our global scope and a reiteration of our two core businesses. We are confident that this emblem will come to represent the same level of professionalism, quality and commitment to our clients that our old logo represented so well in the past.



Corporate Security

In each issue of the newsletter, we will identify, address and comment about issues that are of immediate concern or those that may be on the horizon. In this case, the topic is squarely in both realms. There are ongoing incidents in the best of times, but this problem can be expected to become more severe.

New Location

In January 2009, RMA will celebrate its 21st anniversary. From the sparse beginning in Mike Tucker's spare bedroom, RMA has grown over those 21 years into an established national company that, to date, has worked in 37 states and six foreign countries.

In 1989, RMA moved into its first commercial office space at the Old City Market in Raleigh. This facility was located on the second floor of a newly restored historic market building off Martin Street.

In 1992, RMA moved to the seventh and eighth floors of the Professional Building at 127 West Hargett Street, which was our headquarters for the next 18 years and was the location with which most of you are familiar.

Now RMA has moved into its fourth headquarters facility at 4000 WestChase Boulevard. This building faces Blue Ridge Road and is located north of the State Fairgrounds and immediately south of Wade Avenue. While many of us were somewhat saddened to leave the downtown area, the new setting, location, access and parking are a real advantage to employees and visitors alike.

All of you are invited to come by when you are in the area. The new office is very near the RBC Center, State Fairgrounds and NCSU; only a few minutes from Raleigh Durham International Airport via Business I-40; two minutes from I-40; and just off the Wade Avenue route into Raleigh. Details about our upcoming Open House are coming soon.

RMA Receives 2008 Pinnacle Award

RMA was honored by the Greater Raleigh Chamber of Commerce as a 2008 winner of the RSM McGladrey Inc. Integrity in Business Award. The award recognizes companies that demonstrate dedication to corporate responsibility, integrity and ethics and whose behavior not only benefits their business and employees, but all other like-minded companies. We are extraordinarily proud of this recognition. The Pinnacle Award serves as an acknowledgement of the values and standards that have been a part of our company culture since our very inception.

Workplace Violence: The Gathering Storm

The definition of "workplace violence" has broadened to include two aspects of potential harm to employees. The more classical definition involves the use of violence by an employee or former employee against fellow employees or supervisors. The second and more broad definition includes violence directed against employees from outside sources as result of the course of business such as in armed robbery or assault by customers or clients.

The classic case involves a terminated employee that returns to the workplace and attacks employees and supervisors. For a long time, RMA has worked with client companies to develop workplace prevention programs and to train supervisors and managers to identify potentially violent personnel. Planning, preparation, and forecasting are the central principles in averting workplace violent events.

In the more broad definition, employees that are assaulted in the course of robberies are considered the victims of workplace violence. RMA has helped clients with security planning, design and training intended to make the potential target environment as safe and secure as possible. This assistance has included training in how employees should conduct themselves during a robbery event in order to minimize their jeopardy as much as possible.

In all these cases, routine security plans and procedures are the foundation of prevention and response to such an event. There are special security needs during terminations, lay offs and downsizing. Many if not most companies take special security actions and increase security awareness during these periods. Robbery prevention planning is usually a norm for financial institutions and other cash-handling businesses, but the intensity of these measures may be increased during periods of heightened threat. In tough financial times, robbery tends to increase, which puts those employees in greater jeopardy of being a victim. Not only is the potential for being victim increase, the level of desperation of the perpetrator would likely increase also.

The nation has entered a period of economic chaos that may be unprecedented. The ramifications and scope are still emerging. Experts are contradictory as to the cause, duration, and outcome of the downturn. There is no sector of the economy that is not or will not be affected. The sequential effects of the recession will reach into almost every industry and business, most likely resulting in market contractions, subsequent reduction in production, transportation, supporting service industries and consumer consumption. This is compounded by the housing crisis with foreclosures and the evaporation of credit.

What does this mean for security professionals as it relates to the potential for workplace violence? Such economic contraction means lay-offs. Employees who lose their jobs are stressed during the best of times. In the current situation, with such a general contraction underway, finding employment elsewhere may be nearly impossible in the short term for all but a few categories of worker.



Many otherwise intelligent people were seduced by easy credit and may be over their limit with credit cards and other consumer credit options, have second mortgages against their home equity that has disappeared with the fall in real estate value, and have no other financial buffers available to them. Then they lose their job.

Those who remain employed and are still being paid are still subject to financial strain. Such stress can lead to increased alcohol use, domestic strife and other critical stressors in potentially violent employees.

As security professionals charged with the safety and security of the workplace, it is a time for reexamining security programs relevant to workplace violence prevention and response.

1. Review or establish a workplace violence policy
2. Assess the current level of training for the threat evaluation group, managers, supervisors, and the WPV awareness level of employees.
3. Review and refine exclusion/lockout and lockdown procedures.
4. Review and refine the security plan – access control, surveillance and alarms.

The WPV training and awareness programs should include training in identifying key behaviors – serious stress indicators, mental instability, and physical violence issues. Established prevention strategies should include a well-written and strictly enforced policy including “zero tolerance” of physical violence in the workplace. Security protocols for scrubbing the access control system, key control, and reclamation and the recovery and integrity of identification devices should be reviewed and refined.

Plans for increased security during terminations is essential, but it is important to remember that most violent retributions by terminated employees occur weeks and months after the actual termination event. These attacks seem to come after the individual’s normal coping strategies have failed and their life situation has further disintegrated. It is highly recommended that some form of tracking of terminated personnel be conducted for a period of time to assess the degree to which they are adapting and succeeding in reorientation of their lives.

The economy is in recession and the degree to which it will worsen and the time it will take to recover are being debated by the best economic and business minds in the nation. The only certainty is that these circumstances will impact corporations, companies and their employees. It is imperative that the prudent security manager take stock of all workplace violence prevention and response plans and programs and increase vigilance and awareness. Hope for the best, but be prepared for the worst.

Recommended Resource: <http://www.peaceatwork.org>

Homeland Security



There has not been an attack by international terrorists on US soil since 9/11/01. Most experts believe, however, that another attack will occur and many predict that it will be catastrophic and possibly involve a WMD.

Terrorism in the United States: What Has Changed for Security Planners Since 9/11/01

Since September 11, 2001, threat of terrorism has become a significant factor in American security planning. Many planners do not understand the nuances of true terrorism and consequently, there have been many doom-sayers and “Chicken Little’s” addressing these new threat problems. Terrorism is nothing more than a highly sophisticated form of criminal or paramilitary attack. The success of these actions on September 11, 2001, and the emerging awareness of the vulnerability of United States’ business and governmental facilities and personnel is complicated only by the nature of our free society.

The definition of terrorism has broadened in popular use to the degree that the term is no longer useful in differentiating among types of threats and types of persons or groups that present a danger. In order to clarify the issue, this discussion will utilize a narrow definition of terrorism and differentiate it from other forms of attack. In this manner, security planner and those personnel who implement aspects of such plans can more specifically categorize vulnerability and risk with regard to the nature and intent of entity planning and carrying out such activity.

Central to the definition of *terrorism* is the concept of fear being the effect or objective of the activity. Violence per se is not terrorism unless the intended effect is to instill fear as the primary result. This fear may be used then as a tool for achieving secondary or more oblique goals, most notably being alignment with or acquiescence to a desired behavior or belief structure.

RMA has taken the position since immediately after the 9/11/01 attacks that a security manager cannot interdict or prevent terrorist attack. Private security practices terrorism defense, not counterterrorism. Terrorism defense is a more precise use of the well-established security procedures and technical applications used before the attacks. An RMA consultant wrote this article shortly after 9/11 and we believe that it is still as relevant today.

Revolutionary literature of the 1960's defined terrorism as "the use of or threat of violence to destabilize the sense of wellbeing within a population and erode confidence in the ability of established authority to provide for their safety and welfare." Terrorism was a necessary precursor to guerrilla warfare because it preconditioned the population to support and protect irregular forces by breaking the dependency and confidence bonds between the population and the established government. Fear becomes an effective tool for alienating the leadership from the population over which they preside. Violent actions to assassinate leaders or destroy facilities are not terrorism unless the goal of such acts is to create an environment of fear which in itself will achieve or contribute to an outcome.

Any form of threat or violence may be used as a tool, but the techniques and tactics employed will vary somewhat from those employed when the desired effect is something other than terrorism. Sabotage for example has as its goal the destruction of property or substantial disruption of productive activity. A measure of the success of an act of sabotage would be the monetary loss associated with the event. The tactical and technological aspects of a sabotage plan would focus on different parameters from that of a terrorism plan to attack the same facility. It is these differences that define the importance of understanding terrorism as a unique format of violence.

Protection against crime, sabotage, and terrorism all begin with the same fundamental security axioms. Access control, surveillance and accountability are the fundamental tools for securing a facility and identifying aberrant behavior characteristic of a potential threat. In planning to overcome or compromise a security system, the specific details of an operation are derived from and dependant upon the requirements to achieve a specific desired effect. A terrorist attack need not result in large monetary damages like those desirable in a sabotage attack. Conversely, producing such intense fear and its subsequent coercive effect usually require much more precision, sophistication, and care in the planning and implementation of the action.

A successful terrorist attack might cause relatively little physical or monetary damage but affect the comfort and sense of stability of a large group of people. An act of sabotage must cause significant loss or disturbance to be successful but the effect may be extremely localized. Criminal attacks focus on narrow, specific objectives with no requirement for substantial loss, consequent effect, or residual fear.

Timothy McVeigh is generally referred to in political and media discourse as a terrorist. McVeigh's objective in bombing the Murrah Federal Building in Oklahoma City was not to make people afraid to go to the Post Office in their hometowns. This act was in fact a direct attack on a federal government building in retribution for acts the government had taken that McVeigh sought to avenge. This was not a terrorist attack and McVeigh was not a terrorist. This was an attack by an irregular force on an established government target intended to destroy the facility and kill the federal personnel within. By definition, this was unconventional or guerilla war, one step beyond terrorism on the five-step scale of revolution (Activism - Radicalism - Terrorism - Unconventional Warfare - Conventional Warfare).



This action could have fit well into a terrorist scheme if its intent had been to alienate and separate citizens from government by creating a level of fear that prevented them from visiting federal offices. But in fact, the goal was to kill federal officers in retaliation for actions McVeigh perceived as aggression by the U.S. government.

Today's terrorists are likely to be well financed, focused, and mission-oriented. They are more highly trained, and better organized than ordinary criminals, but they are neither super-human nor super-natural. They are smart, ruthless and diabolical, but as operators they have no capacity beyond that of any other would-be intruder or attacker.

A clear understanding of the specific strategic and operational goals of terrorism enable security planners to more thoroughly examine specific facilities and security programs to assess specific threat and risk of attack. Based on an understanding these subtle differences, measures and countermeasures can be developed or modified to specifically address vulnerabilities. Basic security practices and principles can then be fine-tuned to significantly increase protection against true terrorism.

All terrorism defense measures begin with standard security practices based on fundamental security principles. Therefore, terrorism defense plans must evolve and develop a higher and more elaborate level of security because of the higher capability of trained, organized terrorist operators. But even the most exotic and sophisticated plans to combat terrorist threat will be flawed, however, if they are not based upon and extended from good general security planning and application of basic security principles.

Assessing the threat level for a facility begins with an examination how the facility could fit into the targeting scheme of each type of potential attack. The identification and analysis of manner of attack and choice of weapon level of threat is considered next with regard to how these types of attacks could be most effectively or easily carried out.

The next phase of threat assessment is to ascertain what risk might be present regarding associated factors not directly related to the company or its specific products or personnel. An example of this is the "neighborhood" within which a facility is sited, key personnel live, or materials and product are stored or travel. An illustration of this is the World Trade Center attack of September 11, 2001.

As far as has been determined, none of the companies whose offices were destroyed in these attacks were specifically targeted. They became proximate targets because they were housed in or very near to a major American icon that represented a symbolic target to terrorists. Similarly, the airlines, crews and passengers aboard the commandeered aircraft were proximate victims only because they coincidentally owned, flew or booked passage on the aircraft that eventually were hijacked and used as cruise missiles.

Whether or not company facilities or personnel are direct or proximate victims is irrelevant with regard to outcome, but it is extremely relevant with regard to assessing and analyzing threat and planning appropriate security measures.

Terrorist Threat Assessment Factors

Primary

1. Is the company a symbol or superlative in the public eye in such a nature as to be representative of America, American ideals, or American status or strength?
2. Is this company or facility liable to attract the specific attention of a faction in any issue where violence has been an espoused or demonstrated tactic or strategy?
 - What types of violent acts have been associated with this faction or issue?
 - Is there a specific catalyst or trigger for these incidences of violence?
 - What have these factions said was their intention in using violence as a tool?
 - What were the direct and indirect results of these actions?
 - Were these operations considered successful in achieving the goals of the faction?
3. Is the nature of the company facility, materials or operations consistent with or susceptible to the creation of large-scale or spectacular incidents?
4. Are there individuals within the company whose death would result in major problems or failures for the business, create extensive media and public interest, or who might be considered as icons in any way?
5. Is any national security related activity conducted at the facility?

Proximate

To establish the proximate threat exposure, the direct threat survey may be applied in total or in part to all adjacent or near proximate facilities. The survey should be used also on all facilities that are used, occupied or visited extensively by company personnel. Threat intensity may be mitigated by assessing the variables of distance, intensity of activity and frequency of exposure.

Assessing and Addressing the Terrorist Threat

Terrorism is a current threat in many parts of the world. The events of September 11, 2001 brought transnational terrorism to the United States in a catastrophic manner. An examination of these attacks illustrates the insidious and diabolical nature of the true terrorist who is willing to threaten and take innocent lives as the mechanism for the creation of fear among those who are left. These attacks evidence the patient and intelligent manner with which terrorists often plan and execute their operations. Further, the attacks illustrate the vulnerability of a free society to such acts.

Combating terrorism is the function of governments. As has been seen with the United States' approach following 9/11/01, war against terrorists must be prosecuted financially, diplomatically and militarily in the initial phase and additionally on economic and social fronts in the longer term. Corporations, companies and individuals are neither politically and diplomatically positioned nor financially and militarily equipped to fight terrorism on a macro scale. Just as with ordinary crime, the only defense that an individual entity has is to make themselves or their facility and personnel less vulnerable to attack and in this way deflect the calamity toward less prepared and more vulnerable neighbors. Terrorists are like criminals in that respect. The need for success drives them toward the softer targets. The only practical and achievable defense is to become a harder target than others around you.

Understanding the enemy, how he acts and what he wants to achieve makes it possible to design measures and countermeasures that make a potential target more trouble than its worth relative to other potential targets in the same arena. It is a proven tactic in nature whereas some species have learned to make themselves less attractive as prey than the other species around them.

It is certainly disquieting to divert potential harm away from yourself and toward others, but in confronting reality in the terrorist theater, it becomes the survival of the fittest.

Security Technology

This article was written by RMA Senior Associate Darren Nix.

Darren is on the Editorial Advisory Board of Security Products Magazine. This article and an interview were featured on the web-based Safe and Secure Channel. He spearheads RMA's federal contract work. He is a US Navy veteran and was regional manager of an electronic security service company prior to joining RMA.

Electrical Utilities: Preparing for the Ordinary Means Protection for the Extraordinary

Increased security at Electrical Utility companies for the prevention of ordinary events also provides protection for the extraordinary events. There has been a tremendous focus on protecting our nation's infrastructure from terrorist attacks. For several years, many in the security industry have even been "holding their breath" waiting for terrorist attacks to become routine on US soil. Public agencies and private sector businesses have been preparing for such events and how to mitigate them and/or respond; rightfully so, because it is critical that our industry, and America as a whole, is prepared for such events. The fact is, when conducting a threat assessment of an electrical utility facility, a terrorist attack is considered a low probability event but potentially very critical. Notwithstanding, there is a definite correlation between electrical companies providing increased protection and response to the higher probability lower criticality events and the security measures to protect and respond to terrorism attacks on our infrastructure. As a key element to our country's infrastructure, electrical utilities face the threat of high probability events as well as low probability terrorist acts.



Electrical utility providers have a responsibility to protect a variety of facilities and assets, such as power plants, operation centers, remote maintenance facilities, substations, transmission lines, and office buildings. Each of these facilities holds assets to be protected, such as employees, confidential company files, critical production equipment, precious metals, service equipment, money, and others. Homeland Security directives require electrical utilities to identify, prioritize, and protect BCI (Business Critical Infrastructure) facilities and operations. The utility providers protect assets at these facilities and other assets throughout their organization. A breakdown of those facilities might look like the following:

- Generation facilities including control rooms at these facilities
 - Coal (fossil fuel) plants
 - Hydro Plants
 - Nuclear Plants (Government Regulations on security)
 - Gas fired IC Turbine facilities

- Operations
 - Substations (Some are more critical than others with 500kV subs generally the most critical. Others are 230kV, 115kV, and 66kV Some substations provide power to customers, such as, military bases, hospitals, government facilities, etc.)
 - Transmission lines (hardest to protect)
 - Distribution lines
 - Control Center (very critical facility where generation operations are monitored and to a great extent controlled)

Federal, state, and industry regulatory demands are placing increased pressure on the electrical utility industry to handle incidents in a manner that minimizes the impact of downtime while maintaining public confidence. As with other businesses, utility providers should determine the probability and criticality of specific events with a detailed Threat Assessment. Once this assessment has been completed, the company can then provide the appropriate resources to lessen the possibility of the event or the impact to the company. For example, consider the high probability of copper theft. With the rising cost of copper, there is an increase in theft of copper products. Electrical utility providers are one of the most susceptible victims to this type of theft. In most locations, preventing copper theft is a daily requirement. Thieves have been so bold as to even cut live or electrified copper lines out of substations. In some cases, assailants have lost their lives in the act. A copper theft of this nature could obviously cause some power outages and would draw the public's attention to the company's security. There are certainly many other events to consider, and with the increase of this and other types of incidents in recent years, utility companies have taken many necessary measures to enhance their security programs to prevent higher probability events.

A common standard of care and security practice for the electrical utility companies is to prevent, prepare, and respond. First, prevention techniques are utilized. Each of the following security tools is incorporated in many cases at the facilities:

- Fencing (height, top guard, etc.)
- Lighting (standards)
- Security management systems
- Access control
- Video surveillance and recording
- Intrusion detection systems (buildings, fencing, etc.)
- Signage
- Barriers (natural and man-made)
- Security Guards (presence)
- Hardened control rooms

By creating a security atmosphere around the facilities and utilizing many of the above tools, the companies are essentially attempting to prevent and thwart unwanted events. By creating barriers around the facility, installing fences, adding signage, meeting lighting standards, and using some of these other tools, utility companies are accomplishing two things. First, they are making it more difficult for would be attackers to carry out their plan. With some of these other tools, such as security management systems, intrusion detection systems, and video surveillance, security personnel are able to better monitor facilities. These systems send notifications that would allow security personnel to assess the situation and perhaps intervene prior to the event taking place.

As in our example of the higher probability of copper theft, these prevention techniques also effectively assist in making it more difficult for terrorists. For example, a utility company was experiencing an increase in copper theft at their operations facility by individuals compromising the fence at the back of the facility. Company management elected to increase security by making improvements to the fence, adding video surveillance on the fence line, and implementing video analytics to notify security personnel of activity around the fence. Applying these tools not only makes it more difficult for a copper thief to breach the fence line, but it also makes it harder for a would-be terrorist to breach the fence as well.

Secondly, these companies must be prepared. Preparation unifies and permeates prevention and response. Along with the prevention tools mentioned above, these companies should have fundamental written security policies and procedures. Also, it is extremely critical that they have an Incident Management Plan (IMP) and/or Business Continuity Plan (BCP). After an event or natural disaster, the company must be able to quickly return the business critical infrastructure facilities to an operational status. This accomplishes two things: customer and public confidence is maintained and power production and transmission are quickly returned providing minimal losses in revenue. As companies are implementing these prevention methods, they are basically being prepared. They build on that by training personnel to be prepared. Some of this training is directly related to responding to events. For example, security guards and other personnel are trained in how to respond to certain incidents and how to resolve any problems. Therefore, the preparations made link the level of and methods of prevention and response.

How a company responds to certain events displays how prepared they were to deal with it and the effectiveness of their IMP or BCP. If the response is poor then public scrutiny is almost certain, but even with an effective and well planned response, public opinion is often critical and long lasting. Therefore, prevention and preparation is equally, if not more important, than response. Utility companies must also communicate with local authorities in order to effectively coordinate response activities. For example, if a copper theft has occurred, then security personnel must gather as much of the investigative material possible to give to law enforcement. This may include recorded video, event data, eyewitness statements, and other information that will help in the investigations. Ultimately, the relationship and communication efforts that utility companies develop with law enforcement on the day-to-day, higher probability cases such as copper thefts will increase their overall effectiveness in responding to more critical incidents like terrorist attacks.

Higher probability prevention ultimately assists the company and their security program in being prepared to prevent and potentially respond to terrorist attacks. This point is not meant to imply that if a company addresses all high probability, low criticality events they will be prepared to deal with very critical events, such as terrorist attacks. The resources needed to be able to respond to more critical events are much different than those needed to respond to a less critical event. However, as these companies increase their security posture and implement the tools and techniques to prevent the more probable and most likely less critical incidents, they are ultimately increasing the ability to prevent terrorist activities, are better prepared to deal with terrorist acts, and have the means to respond to those types of incidents.

Feedback

Our goal in producing this newsletter is to provide timely, useful information to our clients in matters of security. We need your help to make this newsletter informative and appropriate. Thank you for taking the time to answer these questions. If you would like more information about a security topic or if you have any questions, please contact us at (919) 834-8584.

1. What type of business are you?
2. Does your organization have a dedicated security department? If not, under which department are security responsibilities?
3. What are your organization's current security challenges?
4. What is your organization's greatest security challenge?
5. Has your organization's attitude about security changed in the last year? If so, how?
6. What security programs or plans are now underway or being considered for the future?
7. What information would you like to see in a security newsletter?
8. How often would you like to receive this newsletter?
9. Would you like to receive this newsletter via email? Is PDF an acceptable format?
10. Please provide any additional comments.

Any for-profit reproduction or distribution of this newsletter or selected parts is prohibited.
For copyright issues or permissions, contact Risk Management Associates